# Propuesta de los documentos administrativos para la Creación de un Centro de Respuesta a Incidentes Cibernéticos para la empresa caso de estudio Cibersecurity de Colombia LTDA

**JAIDUR CANO VARGAS**

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA**
**ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA**
**ESPECIALIZACIÓN SEGURIDAD INFORMÁTICA**
**BOGOTÁ DC. - CUNDINAMARCA**
**2020**

# Propuesta de los documentos administrativos para la Creación de un Centro de Respuesta a Incidentes Cibernéticos para la empresa caso de estudio Cibersecurity de Colombia LTDA

**JAIDUR CANO VARGAS**

**Anteproyecto presentado como propuesta de trabajo de grado, para obtener el título de especialista en seguridad informática**

**ASESORA**

**INGENIERA YENNY STELLA NUÑEZ**

**UNIVERSIDAD NACIONAL ABIERTA Y A DISTANCIA**
**ESCUELA DE CIENCIAS BÁSICAS, TECNOLOGÍA E INGENIERÍA**
**ESPECIALIZACIÓN SEGURIDAD INFORMÁTICA**
**BOGOTÁ DC. - CUNDINAMARCA**
**2020**

## DEDICATORIA

Este proyecto está dedicado a Dios por siempre estar conmigo y permitir mantenerme en pie frente al cumplimiento de mis metas y a mi familia quien siempre me ha comprendido y apoyado en todo el transcurso de mi vida, dándome el aliento que siempre he necesitado para llegar donde estoy en este momento.

## AGRADECIMIENTO

Agradezco a la Universidad por brindarme las herramientas necesarias en la búsqueda del conocimiento orientado a la seguridad informática y en la resolución de problemáticas que afectan la comunidad, haciendo énfasis en la aplicación de la ética y los buenos principios que rigen la sociedad.

También le doy gracias al Ingeniero Luis Fernando Zambrano, asesor y tutor de la materia proyecto de grado I, por su paciencia, tiempo y compromiso demostrado durante todo este periodo, donde siempre estuvo atento a cada duda o corrección que se presentara.

De igual forma mi agradecimiento sincero a la Ingeniera Yenny Stella Núñez, asesora del proyecto de grado, quien me brindó su apoyo y conocimiento para mejorar durante la trayectoria que trazo el diseño del presente documento.

## RESUMEN

Los delitos Informáticos han tenido un incremento exponencial en los últimos años según el portal BC Noticias “El Ministerio de Defensa manifestó que a finales del 2018, los delitos informáticos aumentaron en un 40%, incrementándose en 6.404 casos denunciados ante las autoridades.”[1], afectando a miles de empresas y generando millones de pesos en perdidas, es allí donde entran los CSIRT a jugar un papel indispensable en la protección de la información, a través de planes que identifiquen las vulnerabilidades, controlen y mitiguen el riesgo que se puede sufrir en un ataque informático, de igual forma, creando técnicas que eviten la realización de un nuevo ataque por la misma causa.

Debido a esto se hace necesario crear los documentos administrativos para simular la creación del CSIRT para la empresa caso de estudio Cibersecurity de Colombia LTDA., los que darán soporte a todo el proyecto, como son las políticas, procedimientos, catálogos de servicios, etc. Lo anterior se ejecutará a través de la investigación aplicativa, con fuente de información como el estudio en caso, utilizando la metodología de objeto de estudio y apoyándose de la investigación descriptiva y la recolección de información con entrevistas.

Con lo anterior se espera cumplir con el tiempo establecido de 9 meses para tener listos los documentos requeridos con la siguiente información:

- La situación actual de Colombia en los últimos tres años respecto a la CiberSeguridad.
- El estudio de la factibilidad del proyecto y en que entornos ejercerá el CSIRT
- El análisis de los ataques más comunes, identificando métodos, clasificación y forma de actuar
- Los servicios que se prestaran y de qué forma se ejecutaran
- Los perfiles de los integrantes del CSIR, junto con sus funciones
- Manual de políticas y procedimientos operacionales
- La estructura orgánica del CSIRTs


1. BC. Noticias, “En 2018 se reportaron 11.529 casos de incidente informáticos en Colombia.”, {EN línea}, {14 de mayo de 2019} disponible en: (http://www.bcnoticias.com.co/en-2018-se-reportaron-11-529-casos-de-incidentes-informaticos-en-colombia/)

## PALABRAS CLAVE

CSIRT, Seguridad, Información, Incidente, SGSI

## ABSTRACT

Computer crimes have had an exponential increase in recent years according to the BC News portal “The Ministry of Defense reported that at the end of 2018 there was a 40 percent increase in figures related to computer crimes, which went from 15,962 in 2017 to 22,366 cases registered by the authorities. This was revealed by the Minister of Defense. ”1, affecting thousands of companies and generating millions of pesos in losses, is where the CSIRT enter to play an indispensable role in the protection of information, through plans that identify vulnerabilities, control and mitigate the risk that can be suffered in a computer attack, in the same way, creating techniques that prevent the realization of a new attack for the same cause.

Due to this, it is necessary to create administrative documents to simulate the creation of the CSIRT for the case study company Cibersecurity de Colombia LTDA., Which will support the entire project, such as policies, procedures, service catalogs, etc. The foregoing will be carried out through the application research, with a source of information such as the case study, using the methodology of the object of study and based on descriptive research and information gathering with interviews. With the above it is expected to meet the established time of 9 months to have the required documents ready with the following information:

- The current situation of Colombia in the last three years regarding Cybersecurity.
- The study of the feasibility of the project and in what environments the CSIRT will exercise
- The analysis of the most common attacks, identifying methods, classification and way of acting.
- The services that will be provided and how they will be executed.
- The profiles of the members of the CSIR, together with their functions.
- Manual of policies and operational procedures.
- The organic structure of the CSIRTs

**KEYWORDS**

CSIRT, Security, Information, Incident, ISMS

## CONTENIDO

Pág.

## LISTA DE TABLAS

Pág.

## LISTA DE FIGURAS

Pág.

## LISTA DE ANEXOS

Pág.

No hay lista de anexos

# 1. INTRODUCCIÓN

El presente proyecto se realiza luego de una planeación organizada y detallada, donde se busca cumplir con los requerimientos de documentación en la creación de un CSIRT para la empresa caso de estudio CIbersecurity de Colombia LTDA, lo cual conducirá a hacer frente a las grandes problemáticas de seguridad contra la informática que existen, ya que los ataques cibernéticos han evolucionado, implementando nuevas formas de llegar a la información con aplicativos avanzados y sin ningún tipo de apuro por las víctimas, consiguiendo secuestrar, eliminar o modificar la información de una o más personas.

Los delitos informáticos se han transformado en un problema que está afectando a muchas personas, generando pérdidas millonarias, traumas físicos y psicológicos, puesto que no es el solo hecho de ingresar a un computador y sustraer datos, esto va más allá, se han presentado casos donde el delincuente publica datos privados de víctimas que han preferido terminar con sus vidas antes de hacer frente a la situación. Debido a casos como el anterior surge la motivación de este proyecto, que busca contrarrestar el actuar delictivo, encontrando un salvavidas para todas las personas que hacen uso de la tecnología.

## 2. PLANTEAMIENTO DEL PROBLEMA

¿Los documentos administrativos a crearse contribuirán a dar desarrollo a las actividades propias de un CSIRT como responder ante incidentes y vulnerabilidades?

Los delitos informáticos son acciones antijurídicas que van en contra de los activos de una organización o persona, buscando obtener ingresos ilegítimos al sistema, acceder a la información que fluye por las empresas y ya sea venderla, secuestrarla, eliminarla o cambiarla, lo que puede desencadenar en pérdidas monetarias, dudas en la imagen y hasta la quiebra de la organización.

Según el portal Enter.co "cada día se ve la aparición de casos cibernéticos innovadores, los cuales toman por victima a ciudadanos y empresas, siendo una cuarta parte a plataformas financieras, de la misma forma, se incrementan los robos a tarjetas de crédito en el doble que el año pasado y así mismo todos los demás delitos informaticos"[2].Con esta estadística se puede constatar el riesgo que se corre cada día con los activos, siendo necesario utilizar acciones de protección que permitan una seguridad plena de la estructura del sistema.

Con la creación de la documentación se podrá consolidar el desarrollo del CSIRT buscando brindar seguridad a los clientes, ofreciéndoles servicios de análisis de riesgos, identificación de amenazas y vulnerabilidades y adecuación e salvaguardas. De esta forma se reducirá la estadística en un 2% de las 28.989 estafas realzadas en el 2018, según el portal El Nuevo Siglo en entrevista con el General de la Policía Jorge Luis Vargas (Director DIJIN)

2. Arias. D, "Colombia, el país con más ramsonwareen Latinoamérica, 2018", {EN línea}, {15 de mayo de 2019} disponible en: https://www.enter.co/especiales/empresas/colombia-ataques-ciberneticos-18/

# 3. JUSTIFICACIÓN

La presente propuesta de proyecto se realiza como opción de grado para la especialización de Seguridad Informática, creando la documentación indispensable en la elaboración de un CSIRT, lo cual permitirá reducir los ataques informáticos y a su vez minimizar las consecuencias que puedan generar, implementando técnicas nuevas en contra de los ciberataques.

El CSIRT de la empresa caso de estudio Cibersecurity LTDA. Podrá articularse con los demás centros existentes en Colombia, pudiendo intercambiar conocimiento, aprendizajes y así desarrollar habilidades para contrarrestar los avances de la criminalidad informática.
Se toma el proyecto aplicado porque permite llevar el conocimiento adquirido en la UNAD a solucionar problemáticas que afectan la sociedad, como son los delitos informáticos y los efectos ellos causan, de igual forma en lo personal se desarrollaran habilidades en la parte investigativa, analítica y se ganara experiencia para futuros proyectos.

Algunos CSIRT en Colombia:

- COLCERT (personas encargadas de atender de forma urgente las amenazas cibernéticas en Colombia)
- CSIRT de la Policía Nacional
- CSIRT financiero de ASOBANCARIA
- CSIRT del gobierno de Colombia
- CSIRT-CCIT (eje cuyo fin es atender incidentes de seguridad informática colombiana)

First (Forum of Incident Response and Security Teams), foro global de respuestas a ataques y amenazas informáticas, es la principal organización que ofrece una membresía, la cual permite actuar de una mejor manera frente a incidentes, ya sea, previniendo o reaccionando.

Este líder mundial en seguridad informática reconoció como uno de los mejores oponentes a la delincuencia informática en el 2018 al Centro Vasco de Ciberseguridad por su gran apoyo en pro de la seguridad digital y sus aportes en la protección de la información.

En el 2017 fue el turno del CSIRT de CEDIA del Ecuador, debido a su respuesta rápida y eficiente frente a los diferentes ataques, amenazas y vulnerabilidades presente en el entorno tecnológico.

## 4. OBJETIVO GENERAL

Crear los documentos administrativos para la consolidación de un Centro de Respuesta a Incidente Cibernéticos para la empresa Cibersecurity de Colombia LTDA.

## 5. OBJETIVOS ESPECÍFICOS

Especificar el contexto en el cual está ejerciendo sus actividades el CSIRT y bajo qué parámetros de seguridad opera, a través de un completo análisis de la situación delictiva, para poder brindar un servicio más acertado y eficiente a los clientes.

Esquematizar de forma detallada los servicios en prevención y corrección de seguridad que prestara el CSIRT.

Precisar los perfiles y requisitos que deben cumplir los integrantes del núcleo laboral que harán parte del CSIRT.

Definir las normas, políticas, estándares y procedimientos operacionales que permitirán un normal desarrollo del CSIRT.

# 6. MARCO REFERENCIAL

## 6.1. Marco Conceptual

Seguridad: estado por en el cual no corre ningún tipo de riesgo físico, ni material.
Activo: es un bien que pertenece a una persona o empresa, con equivalencia al dinero.

CSIRT: (Computer Security Incident Response Team), Centro de Respuesta a Incidente Cibernéticos, grupo de expertos en seguridad que actúan de forma preventiva y reactiva ante una amenaza o riesgo.

Informática: rama que a través de procedimientos y técnicas digitales transmiten información ya procesada y almacenada

Tecnología: conjunto de herramientas de la ciencia y la ingeniería que buscan solucionar inconvenientes.

Ataque informático: tentativa de una o varias personas de realizar un daño a un sistema cibernético

Vulnerabilidad: debilidad presente que facilita el actuar delictivo.

Amenaza: evento o persona que puede causar un daño en un activo.

Riesgo: consecuencia que le puede ocurrir a un activo debido a una amenaza.

Salvaguardas: procedimientos tecnológicos que reducen o eliminan un riesgo

Técnica: conjunto de métodos o procedimientos que se acoplan para conseguir un fin determinado.

Política: normatividad legar que se realiza de forma escrita que busca aumentar la seguridad en la organización

Buenas prácticas: procedimientos comprobados que han demostrado resultados satisfactorios en el cumplimiento de determinados objetivos.

Controles: actividades que se utilizan para el normal funcionamiento de un esquema.

Remediación: actividad que se realiza buscando contrarrestar un incidente o una falla en el sistema

Tratamiento: método que se le aplicara a los riesgos hallados en una estructura tecnológica

Mitigar: reducir o disminuir un daño generado por una amenaza contra los activos de la empresa

Informe técnico: documento que compone todo el procedimiento realizado, incluyendo hallazgos, debilidades, fortalezas y recomendaciones

Auditoria: revisión o análisis que se aplica a un determinado esquema informático para conocer las fallas o fortalezas que presente

Firewall: aplicación informática que protege el paso de un ordenador a la red, protegiéndolo de códigos maliciosos

Antivirus: programa de seguridad que se instala en un dispositivo para cuidarlo de aplicaciones maliciosas

Procedimiento: pasos o método que se realizan para el cumplimiento de un determinado objetivo

Sistema: conjunto compuesto por usuario, hardware y software que permite almacenar, procesar y generar una respuesta

Base de datos: es una compilación de datos ordenados que permite a un software utilizar y disponer de ella de acuerdo a la programación que posea

Pen testing: (Test de penetración), pruebas que se realizan a un Sistema para verificar que vulnerabilidades tiene y como se pueden corregir

Malware: Según la organización Avast “aplicación con código malicioso que busca afectar un sistema o una red en busca de un objetivo específico”[3]
Intruso: Persona o software que ingresa a un sistema sin los privilegios o permisos adecuados.

Contraseña: Código compuesto por una serie de caracteres que solo es conocido por su dueño o administrador, con lo cual se ingresa a una determinada ubicación.

Virus: Aplicación que, al instalarse en un dispositivo, cambia el normal funcionamiento del sistema

Usuario: Persona que utiliza un dispositivo electrónico, junto con todos o una parte de sus servicios.

Protección: Cuidar de que un elemento o persona sufra algún perjuicio.

Privilegios: Autorizaciones que se conceden a un usuario para permitir la utilización de servicios.

Encriptar: Cambiar de forma parcial o total la información, utilizando código secreto y llaves de encriptación

TI: Toda la parte tecnológica de una organización, que incluye la parte física, lógica, personas, áreas y demás componentes que permiten el normal funcionamiento y cumplimiento de los objetivos informáticos. [4]

Metodología: conjunto de procedimientos formales y demostrados, que indican la forma de cómo se debe hacer una acción.

Estándar: Modelo o patrón formal y escrito que sirve como punto de partida al momento de aplicarse

Modelo: Patrón que sirve de referencia en la ejecución de un procedimiento, usualmente se encuentran escritos.

## 6.2. Marco Teórico

### 6.2.1. Contextualización Global

Los CSIRT se han desplazo a lo largo de todo el mundo, estando muy presentes en especial en países con mayor desarrollo tecnológico, quienes se han enfrentados a una serie de ataques informáticos que han conllevado a perdidas monetarias millonarias y viendo vulnerados sus sistemas.

Como ya se ha dicho, los equipos de reacción se han creado a raíz del déficit de seguridad informática por parte de las autoridades, quienes han realizado su mayor esfuerzo, mas no es suficiente para el alto volumen de incidentes que se presentan en un día a nivel global.

La seguridad informática es un asunto de interés mundial, es por esto que países como España ha colocado su mayor empeño en hacer frente a los diferentes incidentes cibernéticos, apoyándose en los 53 CSIRTs reconocidos que crearon una red de protección informática para proteger todo el país, cooperando entre ellos para mitigar los riesgos que conlleva cada ataque, en pocas palabras, el país completo está tratando de blindarse por todos los frentes cibernéticos, contando con todos los sectores (financiero, tecnológico, bancario, comercial, etc.). Constantemente se reúnen estos grupos para tocar temas importantes como son, el estado de la seguridad en el país, requerimientos, avances en los ataques y en los métodos de defensa, entre otros., el foro CSIRT.es consolida y guía a todos los grupos, creando pautas que beneficien a todos y constatando que los integrantes de este grupo realmente ofrezcan los servicios de reacción ante incidentes.

Por otro lado, tenemos a los Estados Unidos, quien cuenta con alrededor de 87 CSIRTs registrados en la comunidad administrada por National CSIRTs en todo el país, quienes tienen la responsabilidad de responder ante cualquier incidente informático contra la nación, además trabajan de la mano de CISA (Agencia de Seguridad de Ciberseguridad e Infraestructura). EE.UU. también cuenta con un grupo de CERTs a nivel mundial, con cerca de 52 equipos donde se encuentran dependencias como La Armada, La NASA, Fuerza Aérea, entre otros y países como Brasil, Holanda, Noruega, Polonia, Portugal Rusia, Eslovenia, Suecia, España, etc. organización que labora todos los días del año (24/7), recibiendo miles de denuncias todos los días, tanto por vía digital como física.

Japón siendo el país con mayor nivel de seguridad informática en el mundo, luego de realizar un análisis minucioso respecto a este tema, llegó a la conclusión de que

un solo CSIRT o CERT se queda corto frente a todo el flagelo de los delitos informáticos, por tal motivo impulso una serie de medidas para fomentar la creación de los grupos de reacción a nivel país, alcanzando un total aproximado y registrado de 387 equipos, quienes se consolidaron a través de Nippon CSIRT Association, creando una serie de procesos y actividades estándares, haciendo que todos hablen el mismo lenguaje y puedan intercambiar información y retroalimentarse constantemente, así mismo se asignaron roles, desafíos, capacitaciones, entre otros.

Caso contrario, encontramos en Nigeria, catalogado como el país más inseguro cuando de ataques informáticos se trata, viéndose justificado en la cantidad de CSIRT registrados con que cuenta, uno, así es uno solo, dependiendo directamente del NG-CERT, equipo de reacción del estado quien trabaja de la mano de NCC (Comisión de Comunicaciones de Nigeria), viéndose extremadamente escaso de equipos de reacción si tenemos en cuenta que es el séptimo país más poblado del mundo, con 206.000.000 de habitantes aproximadamente y donde más casos de Spam se presentan cada día.

A lo largo del mundo encontramos países que le han puesto el ojo a la importancia de la seguridad informática, no solo a reaccionar ante incidentes, sino a prevenirlos, creando múltiples equipos (CSIRT, CERT, Áreas Ti, Centros cibernéticos, etc.) que se enfocan en la protección de la información y los diferentes activos tecnológicos de las organizaciones, el grueso de ellos identifico el valor de luchar en grupo, ingresando a asociaciones globales que permiten tener un mayor alcance y efectividad al momento de prevenir o mitigar un determinado ataque, apoyándose de metodologías y estándares que facilitan y orientan el actuar de los especialistas en seguridad informática.

Una de las asociaciones de respuesta ante incidentes cibernéticos más reconocida es FIRST (foro de equipos de reacción ante incidentes seguridad), el cual constantemente realiza eventos como simposios, conferencias, coloquio y demás, en diferentes países, con esto se puede intercambiar herramientas, información técnica, accionar delictivo, vulnerabilidades, nuevas amenazas, riesgos más altos y muchos otros temas de interés cibernético.

### 6.2.2. Contextualización Empresarial

A consecuencia de la infinidad de ataques que se realizan cada día dirigidos a las empresas, las organizaciones han tenido que blindarse de modo que puedan

proteger la información y generar un ambiente de seguridad sus empleados y clientes, ya que una entidad con reputación de seguridad dudosa muy posiblemente ira a la quiebra.

En Colombia algunas empresas como Asobancaria cuenta con su CSIRT, el cual se orienta en la protección informática de la parte financiera, siendo un apoyo importante en la utilización de la red informática, en la realización de transacciones y el movimiento general de datos, sensibilizando cada entidad para que entiendan que la seguridad cibernética es compromiso de cada integrante de la empresa.

Instituciones públicas también cuentan con su grupo de reacción, entre ellos el CSIRT de la Fiscalía y de la Policía, donde cualquier usuario puede hacer una denuncia, obtener información y enterarse de las últimas noticias sobre ataques informáticos, también esta ColCERT del Ministerio de Defensa, orientado a la seguridad cibernética a nivel público y privado, estos portales brindan servicios gratuitos de prevención y reacción ante incidentes.

Así mismo, existen empresas que no crean su propio grupo de protección, sino que contratan terceros que apliquen esta protección, algunos son Entelgy quien ofrece servicios de CSIRT a empresas como Claro, BBVA, entre otros, también están SWAT Security, IT-SS, Olimpia, Incibe y otros.

En general las empresas han entendido que invertir dinero en proteges sus activos informáticos puede ser la mejor decisión que tomes y así lo piensan la gran mayoría, más aún existen algunas, sobretodo pequeñas organizaciones que no le prestan atención a este tema e imaginan que nunca van a ser víctimas de este accionar delictivo, protegiendo toda la entidad con tan solo un antivirus o firewall que en ocasiones es pirata, son estas las que muy posiblemente en poco tiempo pasaran a engrosar la estadística de las empresas víctimas de ataques informáticos.

### 6.2.3. Avances de los CSIRT

Los equipos de reacción ante incidentes comenzaron a ser ejecutados en 1988, promoviéndose con grupos de personas con amplio conocimiento en el manejo de la informática y programación pero con poca experiencia en procesos donde se hace frente a un incidente de manera inmediata, para evitar o mitigar riesgos, a esto se le suma el poco desarrollo de las herramientas del momento, las cuales no presentaban el avance que tiene hoy en día, ni la facilidad de adquirirlas.

La implementación empezó de la mano de errores y debilidades dentro de los mismos equipos, mas con el pasar del tiempo y las experiencias obtenidas se fueron corrigiendo e innovando en metodologías y técnicas que ofrecen más protección a la información.

Otro punto a favor en el desarrollo, son los antecedentes o record histórico que se han recogido a través de los años, donde se puede retroalimentar e intercambiar información con otros grupos además de la gran cantidad de artículos que se encuentran en internet, al alcance de cualquier persona.

Con la gran demanda que han tenido los CSIRT, se vio la necesidad de orientarlos hacia diferentes entornos, como educativos, financieros, de salud, gubernamentales, comerciales y muchos más, con lo cual se han podido especializar, brindando un apoyo más eficiente y concreto, esto demuestra la habilidad de adaptación que han debido desarrollar para combatir los crackers o hackers sombrero negro.

Definir cuál es el mejor equipo de reacción (CSIRT/CERT) en este momento es muy difícil, pues todos hacer su mejor esfuerzo, alcanzando un nivel muy alto en protección de activos informáticos, sin embargo en el 2015 CyberEx International realizo una competencia a nivel mundial entre treinta y cuatro equipos, alcanzando la mayor calificación el equipo CERTUNLP de Argentina, perteneciente a La Universidad nacional de la Plata.

Los equipos de reacción actuales, implementan una serie de herramientas de alto nivel que permiten prevenir, detectar y eliminar amenazas, al igual que se apoyan de configuraciones y estándares que limitan la influencia de errores, terminando con acciones de mejoramiento o salvaguarda, quienes evitan la perdida de información, aplicativos, estructuras y demás elementos que componen la organización informática de una empresa.

### 6.2.4. Aportes

La Organización Cisco argumenta que:

*"*La red informática ha venido teniendo cambios en los últimos años, tanto en importancia como estructuralmente, saliéndose de los estándares y fronteras establecidos, aumentando su capacidad, rendimiento y también sus vulnerabilidades, convirtiéndose en un blanco atractivo para los delincuentes, debido especialmente al flujo de la información que mueve y el precio tan alto que puede costar."[5]. Esta afirmación nos permite entender que no hay un proceso que sea cien por ciento seguro, siempre van a presentarse amenazas que puedan causar un riesgo potencial. Como aporte a la propuesta nos permite tener una vista más objetiva acerca de la seguridad informática, viéndola como un gran reto y evitando actuar de forma confiada frente a las diferentes vulnerabilidades de los sistemas.

Por otro lado, el Fundador de la empresa Microsoft, Bill Gates en una reunión empresarial manifiesta que:

*"*Las personas siempre desean libertad y privilegios en la utilización de la internet, volviéndose más dependientes de los equipos tecnológicos como celulares, ordenadores, etc.*"* [6]. La frase de Bill ratifica que cada día las necesidades tecnológicas de las personas son mayores a la realidad de la seguridad para administrarla. De igual forma el proyecto brinda su mayor esfuerzo para satisfacer los requerimientos técnicos de los sistemas de las organizaciones y las personas en general, protegiendo al máximo el flujo de la información y los activos en general.

5. CISCO, "Seguridad para redes empresariales", {En línea}. {2019} disponible en: (https://www.cisco.com/c/es_co/solutions/enterprise-networks/enterprise-network-security/index.html?CCID=cc000009&DTID=pseggl000015&POSITION=SEM&COUNTRY_SITE=co&CAMPAIGN=sc-00&CREATIVE=CO_SEM_SEC_Security-SPA_PM_NB_-ADW_All-Visitors-Seguridad-&REFERRING_SITE=Google&KEYWORD=seguridad%20informatica&ds_rl=1261909&ds_rl=1261909&gclid=Cj0KCQjwiILsBRCGARIsAHKQWLMXIyH-JjNwcyBSJFuyYAqUFF0xGUVkhURKQGivX2q6Eks7Sf8GUXIaAqKPEALw_wcB)
6. LA NACIÓN, "Bill Gates apuesta por un nuevo sistema de seguridad informática", {En línea}. {2017} disponible en: (https://www.nacion.com/tecnologia/bill-gates-apuesta-por-un-nuevo-sistema-de-seguridad-informatica/RIDPAYNYANEBBI3LM5EPU3WW44/story/)

El empresario y programador informático Mark Zuckerberg luego del escándalo de Cambridge Analytica, expreso:
“Soy el creador de esta plataforma y por ende debo responder por lo que con ella suceda. Vamos a aprender de esta experiencia para asegurar más nuestra plataforma y hacer que nuestra comunidad sea más segura para todos”[7].
Mark enseña la responsabilidad de cada negocio, donde debe haber entrega, compromiso y arrojo para cumplir con las metas predispuestas y dar cumplimiento a los objetivos programados.
El CSIRT de igual forma aplicara el conocimiento adquirido con la experiencia, en todos los procedimientos que realice, para así, poder encontrar vulnerabilidades más ampliamente.

La delegación de la unión europea en seguridad cibernética (ENISA), a través del documento:
Como crear un CSIRT paso a paso. Brinda una gran información acerca de los requerimientos, especificaciones y procedimientos que trae la realización de un centro de estos
Este documento sirve de apoyo al trámite que se debe realizar en la creación del CSIRT, tanto documental como técnicamente.

La organización First (Forum of Incident Response and Security Teams), siendo una de las máximas autoridades en CSIRT a nivel global, manifiesta que:
“Es muy probable que una organización se enfrente a un incidente de ciberseguridad de algún tipo en algún momento de su vida, independientemente del nivel de defensa de ciberseguridad implementado. “[8]
Siendo esto una realidad y viéndose cada día, donde miles de empresas se convierten en víctimas de un sinnúmero de ataques casi a diario, sin importar el sistema defensivo que aplique.

7. MUNDO, ” Zuckerberg rompió su silencio y habló sobre el escándalo de Cambridge Analytica”, {En línea}. {2019} disponible en: (https://www.semana.com/mundo/articulo/que-dice-mark-zuckerberg-sobre el-escandalo-de-cambridge-analytic/561079)
8. FIRST, “FIRST shares 11 vital steps towards cyber security resilience in 2020”, {En línea}, {09 de octubre del 2019} disponible en: (https://www.first.org/newsroom/releases/20191009)

El Centro Criptológico Nacional (de Europa), genero la:
Guía de creación de un CERT/CSIRT. La cual enseña la forma adecuada y los procesos logísticos u administrativos necesarios para culminar con buen fin esta creación. Guía que es una ayuda indiscutible para el proyecto que se está realizando.

La revista País publicó una entrevista con Kevin Mitnick, uno de los mejores hackers del mundo, quien respondió a la pregunta, ¿Actualmente cuál puede ser la amenaza más fuerte que hay?
“La ingeniería social, de la mano de todas las aplicaciones que realizan un mal al sistema forma oculta.”[9]
Demostrando una vez más la necesidad de implementar nuevos mecanismos para enfrentar a la delincuencia cibernética e investigar más a profundidad los taques existentes.

El diario digital El confidencial en entrevista con el criptógrafo y profesor de Harvard Bruce Schneier, también llamado el Gurú de la ciberseguridad, comenta:
“Cuando Corea del Norte atacó Sony. Lo preocupante es que hace unos años estas acciones necesitaban una inversión enorme que solo un gobierno podía financiar. Ahora ya no es así.”[10]
Es decir, los avances tecnológicos han traído ventajas para la sociedad, pero también han creado facilidades para quienes hacen ataques, con tan solo un par de aplicaciones que se pueden explotar en un ordenador de poca capacidad, requiriendo solo el computador y la red de internet, se puede lanzar una ofensiva que puede traer millones de peos en perdida.

9. Molist. M, “La gente no está entrenada contra el engaño a través de la tecnología”, {En línea}, {15 de junio del 2006}, disponible en: https://elpais.com/diario/2006/06/15/sociedad/1150322409_850215.html
10. Elconfidencial, “Tu coche ya está conectado a internet y ahora cualquiera puede usarlo para matarte”, {En línea}, {11 de julio del 2019} disponible en: (https://www.elconfidencial.com/tecnologia/2019-07-11/bruce-schneier-ciberseguridad-iran-iot-corea-norte-click-matarlos-a-todos_2115135/)

### 6.3. Marco Legal o jurídico

Ley 527 de 1999 (Comercio electrónico), normaliza todo lo relacionado a los mensajes de datos

Ley 1273 de 2009, Cuidado de los datos

Ley 1341 de 2009 (Sector TIC), Principios y conceptos sobre la sociedad de la información y la organización de las Tecnologías de la Información y las Comunicaciones

Decreto 1727 de 2009 (Habeas Data), Comunica la forma como debe ser tratada la información personal por parte de los custodios de la misma, en todo momento y con consentimiento del propietario

Decreto 1704 de 2012, manipulación de las comunicaciones

Decreto ley 019 de 2012, Sujetos encargados de la parte digital

NTC ISO/IEC 27005, catálogo de amenazas y vulnerabilidades.

NTC ISO 31000, administración del riesgo.

NTC 5722, exigencias para que las organizaciones cumplan eficientemente con las necesidades en el cumplimiento de la continuidad del negocio

ISO IEC/27031, fundamentos informáticos y conceptos relacionados a la tecnología, buscando dar seguimiento al negocio

ISO IEC/27032, exigencias normativas para la protección de la tecnología informática

ISO IEC/27035, Gestión de incidentes informáticos

ISO IEC/27014:2013, conceptos y principios para el gobierno de la SI.

ISO IEC/38500, norma que brinda conceptos y metas en el cumplimiento de una buena gobernanza

Magerit versión 3, técnica orientada en la gestión de riesgos informativos de una empresa

Octave, la evaluación vulnerabilidades

NIST 800-30/-39, Metodología para la gestión de riesgos

MIPG, modelo integrado de planeación y gestión.

Nist, patrón enfocado en proteger los controles industriales

MISP, Opensource Threat Intelligence Plataform & Open Standards for Threat Information Share
“Compartir información mediante una plataforma de inteligencia de amenazas”.

STIX, TAXII, Cybox, Intercambio automatizado global de amenazas.

Carta magna de Colombia (CNC)

Control Interno (Ley 87 de 1993)

Código Penal (Ley 599 del 2000)

Código Disciplinario Único (Ley 734 de 2002)

CONPES 3854 de 2016)

## 6.4. Marco Teológico

Un CSIRT basa su funcionamiento en la tecnología, es por eso que se hace necesario implementar un conjunto de técnicas que permitan su óptimo funcionamiento, al igual en cada una de las etapas en su creación se debe utilizar herramientas de la ciencia aplicada para su diseño.
Para este proyecto se hace ineludible utilizar algunos componentes innovadores como son:

- Sistema operativo Windows 8, aplicación que direccionará el ordenador con el cual se realizará el proyecto, siendo la principal aplicación con que cuenta el ordenador.

- Sistema operativo Kali Linux, software orientado a la seguridad informática con más de 300 herramientas para hallar vulnerabilidades en un sistema, muy utilizable hoy en día en las auditorias

- Microsoft Office, suite ofimática para la creación y edición de documentos como Word, Excel, PowerPoint, etc., permitiendo dejar un registro de las diferentes actividades y procedimientos que se realizan.

- Cisco Packet Tracer, aplicación para simular entornos de una organización, creando un plano que permite ser editable y funcional de acuerdo a los requerimientos

- VirtualBox, software para crear ambientes virtuales, siendo un gran apoyo, ya que posibilita simular el sistema de información y realzarle ensayos, sin necesidad de afectar el entorno real.

- Pilar, aplicación para realizar análisis de riesgos, brindando un valor a las vulnerabilidades, amenazas y generando salvaguardas para la estructura informática.

- Gooogle Chrome, buscador de información en internet, el cual ofrece enlaces de mucho apoyo en las investigaciones que se requieran.

## 6.5. Marco Contextual

La empresa Cibersecurity se encuentra ubicada en el país de Colombia, Suramérica, orientada a cuidar la información, a través de diferentes procedimientos que permiten identificar, vulnerabilidades, amenazas, riesgos y salvaguardas, de acuerdo a los niveles de contratación de servicios realizados con sus clientes.

Dicha empresa se dispone a crear un CSIRT (Centro de Respuesta a Incidente Cibernéticos), para lo cual requiere una serie de documentos que se realizarán a lo largo del proyecto, estudios referentes a la seguridad informática, guías

procedimentales en la creación de CSIRT y con la pauta del tutor de proyecto de grado.

Utilizando como referencia documentos generados de entidades reconocidas en el medio de la seguridad informática como CISCO, Aseguradora RSA, Centro Cibernético Policial, La delegación de la unión europea para la protección cibernética (ENISA), El Centro Criptológico Nacional (de Europa), Organización Internacional de Normalización (ISO), (COBIT) y otros.

Todo el proyecto se llevará a cabo entre septiembre del 2019 y septiembre 2020.

## 6.6. Marco Espacial

El desarrollo de esta investigación se realizará en el marco de la empresa caso de estudio Cibersecurity de Colombia LTDA, más específicamente, el CSIRT que se creará en dicha organización, el cual tendrá un eje de aplicación en el país de Colombia.

## 6.7. Marco Metodológico

Objeto de estudio
Este documento se diseñará a través del tipo de investigación aplicada, pues esta forma de estudio utiliza métodos, teorías y conocimiento históricos para ser aprovechados en la solución de situaciones en el presente, además se aplica a la problemática ya conocida como son los efectos causados por los delitos informático, quienes atacan directamente los activos ya sean personales o de una agrupación legalmente constituida. Todo esto siempre en busca aumentar la protección de los bienes de los usuarios que navegan en la internet. Así mismo sirve de apoyo en la creación de todo el paquete documental que se necesita para consolidar el desarrollo del CSIRT, basándose en otros proyectos ya fundamentados sobre la misma temática.

Fuente de información
El fundamento académico que se aplicará será estudio de caso, donde se recopilara información y parámetros procedimentales de diferentes autores y entidades que apoyen el proyecto en general, permitiendo hacer una descripción más detallado de

la problemática que se está viviendo en nuestros días referente a los ciberataques, lo cual incluye amenazas, vulnerabilidades, riesgos, activos, salvaguardas y los mismos hackers, quienes manejan una ética muy particular que va en contra de la mayor parte de la sociedad.

Nivel de medición y análisis de información

El método a utilizar es la investigación descriptiva, detallando y aplicando cada componente requerido en el diseño del CSIRT, obteniendo datos reales y científicos acerca de la problemática que afecta la seguridad informática en Colombia, transformando esta contrariedad en un fenómeno que cada día crece exponencialmente y que crea victimas a nivel global, causando millones de dólares en pérdidas.

Extensión de estudio

Se empleará el tipo de muestreo determinístico o no probabilístico, afirmándose en los estudios recopilados y en los requisitos vigentes en la creación de la documentación del proyecto, con este muestreo se permitirá seleccionar un grupo de sujetos escogidos por el investigador que tengan amplio conocimiento en el tema planteado, facilitando la accesibilidad a una información de calidad

Recolección de información

Los datos necesarios para la propuesta se conseguirán por medio de encuesta, utilizando un target con amplio conocimiento en el tema, donde se obtendrán datos sobre experiencias, conocimiento y problemáticas informáticas vigentes, por medio de preguntas cerradas o de selección múltiple, así se podrá crear una estadística que apoya la estructura del proyecto.

# 7. DOCUMENTOS NECESARIOS PARA LA CREACIÓN DE UN CSIRT

## 7.1. ACTIVIDADES DEL CSIRT BAJO UN COMPLEJO ANALISIS DELICTIVO

Especificar el contexto en el cual está ejerciendo sus actividades el CSIRT y bajo qué parámetros de seguridad opera, a través de un completo análisis de la situación delictiva, para poder brindar un servicio más acertado y eficiente a los clientes.

### 7.1.1. Contexto de aplicación del CSIRT

El CSIRT de la empresa caso de estudio Cibersecurity Colombia LTDA. Ejerce sus facultades en cada uno de los clientes que contratan los servicios, mayormente en Colombia, aunque está disponible en caso de ser requerido en otros países, manteniéndose actualizado con los nuevos accionares delictivos que se presenten en contra de la informática, no solo a nivel local, sino también global, permitiendo mantener los parámetros de seguridad con los activos de las organizaciones y ofrecer integridad, confidencialidad y disponibilidad a los datos.

Este grupo de respuesta combina dos tipos de CSIRT, el empresarial con el de soporte[11], ampliando su accionar e innovando herramientas y acciones que permitan ir un paso adelante que los crackers o hackers sombrero negro. Con lo anterior se obtiene algunos beneficios como:

- Focalizar todo el esfuerzo en una respuesta rápida y eficiente que brinde la protección requerida.
- Agilidad en los procesos con el aporte de otros centros que agreguen conocimiento y experiencia en las amenazas que se puedan presentar.
- Aumentar el conocimiento y las capacidades a través de actualizaciones e investigaciones que conlleven a realizar una labor óptima.
- Aportar no solo a los clientes, sino también a toda la comunidad de la seguridad informática, dando aportes que puedan ser utilizados en diferentes partes del mundo.
- Generar confianza en cada uno de los procesos que realice la empresa, demostrando responsabilidad y juicio a sus clientes.

11. Sasia. D, “Gestión de incidentes de seguridad de la información/CERT/CSIRT {EN línea}, {07 de octubre de 2015} disponible en: https://es.slideshare.net/danielsasia/gestin-de-incidentes-de-seguridad-de-la-informacin-cert-csirt

La intención de la empresa caso de estudio CIbersecurity Colombia LTDA. Es afianzarse en el medio de la seguridad informática, a través del CSIRT, ofreciendo nuevos y eficientes servicios a las organizaciones que contraten con ellos, quienes pueden acceder a un soporte relacionado a la protección de sus activos antes y/o de un incidente.

#### 7.1.1.1. Evolución de los grupos de emergencia ante incidentes informáticos

La creación de los equipos que luchan contra los incidentes cibernéticos tiene sus raíces el 02/11/1988 a consecuencia de la aparición de uno de los primeros ataques informáticos del momento, el gusano de internet (Morris), el cual fue detectado y analizado por expertos de la universidad Carnegie Mellon en Pennsylvania, quienes visionaron la gran cantidad de ataques que se vendrían y tuvieron la grandiosa idea de crear el primer grupo altamente entrenado para hacer frente a este nuevo flagelo delictivo. A partir de este momento han venido en crecimiento los grupos de reacción a nivel mundial, ofreciendo una pequeña salida al caos que se presenta con el incremento exponencial de amenazas contra los distintos sistemas informáticos. En América se implementó el ´primer CSIRT en los años 90, como respuesta a los daños que se estaban presentando, quienes trajeron perdidas millonarias y llevaron a la quiebra muchas empresas

#### 7.1.1.2. Impacto

Se considera que los CSIRT han tenido un impacto fundamental a nivel global para enfrentar a los ciberdelincuentes, más el mayor de estos ha sido conseguir la reducción de vulnerabilidades de las organizaciones que hacen uso de él, debido a los análisis que se aplican al comienzo de todo proceso, verificando activos, su importancia, debilidades, amenazas y riesgos, lo cual conlleva a encontrar salvaguardas que permitan mitigar o eliminar las consecuencias de un ataque.

Se puede decir, que el grupo de reacción tiene una actividad proactiva, pues siempre trata de ir un paso a delante de los crackers en pro de asegurar la estructura tecnológica.

#### 7.1.1.3. Ventajas

La implementación de un equipo frente a incidentes informáticos radica en la importancia de poder contar con un grupo especializado de expertos que orienten su accionar en proteger la información de una empresa.

Ofrece una serie de recursos informáticos de software, hardware, configuraciones, monitoreo y capacitación que permitan crear una seguridad robusta alrededor de la protección cibernética.

Brindan asistencia en tiempo real para recuperarse de forma rápida y sin tantas consecuencias de un incidente informático, ya sea ocasionado de forma voluntaria o accidental.

Cuenta con un soporte jurídico que asiste a la organización en temas relacionados con la informática, pudiendo ir de la mano con las leyes y normas que rigen la utilización de la tecnología.

Mantiene un seguimiento constante a toda la estructura informática, teniendo en cuenta cada activo y los cambios sospechosos o anormales que se puedan presentar.
Crea una red informática entre otros grupos dedicados al mismo tema como CERT, CSIRT o áreas TI, que permita intercambiar experiencias y datos importantes para contrarrestar los incidentes computacionales.

Contar con un CSIRT en una organización, eleva la imagen de confianza y seguridad para sus clientes, dando una apariencia de seriedad que catapulta la empresa sobre muchas otras que no hacen uso de estos equipos.

El CSIRT tiene una amplia gama de servicios completos, detallados o específicos, de acuerdo a las necesidades y requerimientos que tengan las empresas y los sistemas de información.
Documenta cada incidente o procedimiento que se realice, evitando que suceda de nuevo, manteniendo protegidos los datos confidenciales e importantes de las organizaciones.

Cada sistema es diferente, es por esto, que lo primero que se debe realizar es un correcto estudio y mapeo del sistema tecnológico que ejecuta la empresa, junto con las personas que operan o tiene accesos al mismo.

#### 7.1.1.4. Necesidades globales

Para nadie es un secreto, que a nivel mundial se está presentando una problemática muy grande que se desprende de la utilización de la tecnología, debido a que cada día son más las empresas que implementan los sistemas de información, moviendo la mayoría de sus activos a través de redes de datos, algunas con más vulnerabilidades que otras, pero todas convirtiéndose en un blanco provocativo para los crackers o hackers de sombrero negro que ven en ellas una forma fácil de obtener dinero sin mucho esfuerzo.

Es aquí donde entran los CSIRT a evitar que se ejecuten estos ataques y crear barreras seguras entre los delincuentes y la información de las empresas y personas del común, contando con que la evolución de herramientas de código libre ha abierto las puertas a muchos bandidos que no tenían ni idea de que eso existía.

#### 7.1.1.5. Necesidades Locales

A nivel país se está presentando un cambio debido a IoT (Internet of Things) internet de las cosas, consistente en automatizar la mayor cantidad de elementos cotidianos en la vida de las personas, esto a primera vista es favorable y aumenta la comodidad de todos, pero si se analiza más a profundidad, se identifican desventajas como la asignación de direcciones IP, obligando a pasar de IPv4 a IPv6, además, se abrirán brechas de seguridad muy grandes que podrán ser utilizadas por delincuentes para acceder a estos nuevos equipos conectados a la red.
En este punto se aplica la formula, entre más accesorios en la red, más protección se va a necesitar, obligando no solo a empresas, sino a algunos individuos a hacer uno de los CSIRT para asegurar sus viviendas y todo lo que en ella hay, pasando de la seguridad física a la lógica.

En general un CSIRT es un escudo que compite contra los delincuentes para evitar que ellos cumplan su cometido, ya sea a nivel global o local, protegiendo pequeños o grandes paquetes de datos y permitiendo que el sistema funcione con eficiencia, seguridad, privacidad, disponibilidades e integridad.

### 7.1.2. Parámetros de seguridad

El CSIRT de la empresa caso de estudio Cibersecurity de Colombia igual que todas las entidades legales del país están regidas por normas y leyes que encaminan el accionar de una forma justa y equitativa, permitiendo brindar un servicio que cumpla todos los estamentos legales

#### 7.1.2.1. Apoyo normativo

- ISO-27035:2012, ofrece una serie de consejos o buenas practicas orientados a la administración de incidentes.
- ISO-27001:2013, se orienta a la adecuada consecución de la seguridad informática, a través de la prevención y corrección de riesgos
- ISO-27002:2015, brinda una serie de controles en pro de incrementar la seguridad informática.
- Magerit Versión 3, metodología orientada a identificar vulnerabilidades, evitar amenazas, mitigar riesgos e idear salvaguardas

#### 7.1.2.2. Análisis de la situación delictiva en Colombia

Los ciberdelitos en Colombia han tenido un incremento del 70% a partir del 2015, informa el Portal Oficial de Estadística TIC, esto debido al acercamiento tan amplio que ha tenido la población colombiana con la internet, ya que con los avances tecnológicos se ha tratado de que la red llegue a todos los rincones del país, lo cual también abrió las puertas para que hackers y crackers empezaran a colocar el ojo sobre esta forma de delito.

En Colombia se cuenta con la ley 1273 del 2009, esta norma fue creada por el vacío jurídico que había respecto a este tema, pero en ocasiones se queda corta, a pesar que la Policía Nacional y la Fiscalía cuentan con grupos enfocados únicamente a la investigación de estos delitos, en ocasiones se quedan cortos, ya que en nuestro país la cantidad de cibercrimen que se presenta es demasiado y de muchas formas.

Dentro de los delitos informáticos más comunes en Colombia están:

- Phishing, este ataque consistente en una estafa que comienza con un correo electrónico malicioso, el cual simula provenir de una entidad reconocida y con un mensaje que hace creer a la víctima que requiere una verificación de datos con un link que al aplicarlo abre un formulario con iconos y logos de la empresa, el usuario inocentemente inserta sus datos como contraseñas, nombres, fechas, etc., los cuales son utilizados por el atacante para suplantar la identidad y realizar compras o transferencias, desocupando las cuentas de las personas.

  En 2017 se presentó en el país la mayor cantidad de víctimas por este hecho, con un mensaje que fingía provenir de la entidad bancaria Bancolombia, convirtiéndose en el segundo país con más ataques a nivel latinoamericano y con pérdidas anuales que superan los seis millones de dólares.
- Ramsonware, ataque consistente en el secuestro de la información ya sea eliminándola o encriptandola y liberación a cambio de dinero. Colombia se encuentra en el primer lugar de Latinoamérica con mayor cantidad de estos casos (según Eset) con un 30%, siendo el más utilizado el denominado Cryisis, quien utiliza la ingeniería social por medio de correos electrónicos referentes a una deuda en mora que presentan las posibles víctimas y al momento de abrir el archivo adjunto, se activa el virus dispersándose por el ordenador y bloqueando la información, posteriormente se muestra una imagen con los datos para pagar y desbloquear los datos.
- Smishing, consiste en un mensaje de texto que llega al celular el cual motiva a las personas a seguir un link o llamar a un número telefónico, manifestando que se han ganado un premio, para aprovechar una promoción o una calamidad ocurrida, luego el atacante por medio de ingeniería social convence a las víctimas para dar información o enviar dinero. Este tipo de ataque se ha empezado a implementar de forma masiva desde el 2017 y ha estado en aumento los posteriores años (según el centro cibernético policial).[12]

12. Caivirtual, “Centro Cibernetico Policía Nacional” {En línea}, {2019} disponible en: (https://caivirtual.policia.gov.co/)

De igual manera existen Malwares como Skimming, Carta Nigeriana, Keylogger, Vishing y otros, todos buscando estafar a las personas y sustraer su dinero, los cuales se han detonado con el desarrollo de la tecnología, pues las personas han tomado confianza en el uso de la internet, pensando que a ellos nunca les pasara y facilitando la información que requieren los delincuentes para hacer efectivos sus ataques.

Por otro lado, encontramos las redes sociales, originalmente creadas para que las personas se conectaran e intercambiaran información, sin ninguna malicia, pero debido al gran auge e importancia que han desarrollado al punto de convertirse en vicio para algunos, se han aprovechado los delincuentes, comenzando a llevar allí los delitos como suplantación o usurpación de identidad, ciberbullyng, Grooming, Sexting, etc.

Según la Dirección Judicial de Inteligencia de la Policía Nacional, nuestro país está ubicado entre los peores en comportamiento digital y genera más riesgos de este tipo, manifestando también que el 66% de sus habitantes han sido víctimas de delitos informáticos, quedando la mayoría impune por falta de denuncias de las víctimas, quienes algunas veces no lo hacen por vergüenza o por falta de efectividad en los procesos de investigación. Debido a esto la Policía de ha valido del sitio WEB https://caivirtual.policia.gov.co (centro cibernético policial), donde las victimas pueden denunciar, recibir consejos y asesorías sobre cómo actuar frente a estos hechos.

La revista el Tiempo en su magazine digital del 30 de octubre del presente año, informa que en Colombia al igual que en el mundo se ha presentado un incremento exponencial en los diferentes ataques informáticos, estando encabezados por el Phishing, la suplantación de identidad, la contaminación con Malware y los demás fraudes digitales que vemos todos los días.[13]. Con el anterior reporte de este importante periódico se ratifica una vez más el imán que está presentando la informática en todo el mundo, atrayendo hackers de todo tipo (sombrero negro, rojo, blanco, etc.), quienes ven en la ciberinformación una oportunidad de hacer dinero fácil y sin dejar huella.

En la siguiente imagen (Figura 1. Estadística Ataques) se puede identificar los principales ataques informáticos que se han efectuado en Colombia

Figura 1. Estadística ataques

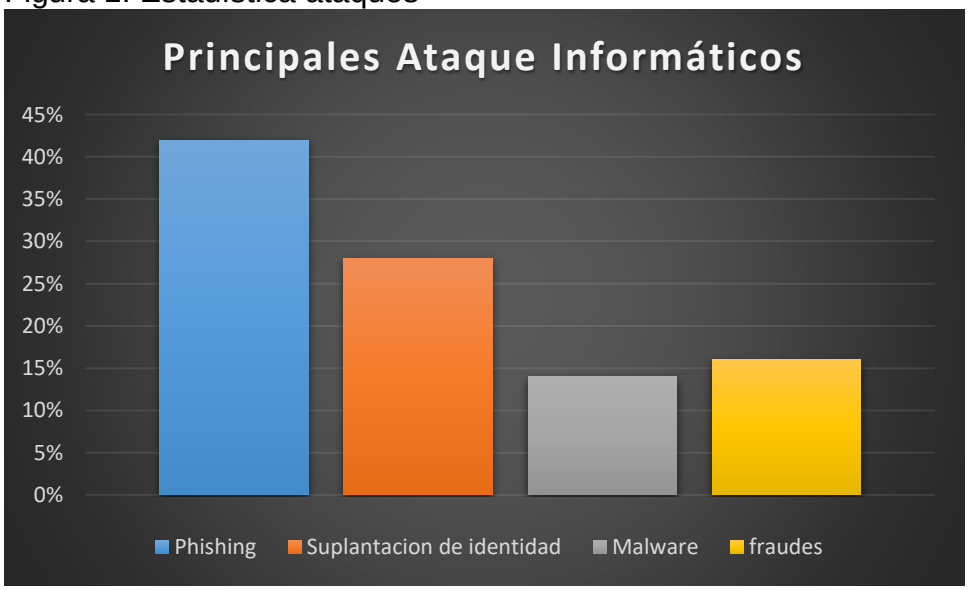



Imagen propia

Datos importantes obtenidos:

- Phishing con un 42%, representa la mayor cantidad de incidentes, recordando que casi a diario llegan correos maliciosos, tratando de hacer que las victimas pierdan su dinero a través de engaños, generando pérdidas millonarias al año.

13. El Tiempo, “En 2019 se reportaron más de 28.000 casos de ciberataques en Colombia”, {En línea}, {30 de octubre del 2019}, disponible en: (https://www.eltiempo.com/tecnosfera/novedades-tecnologia/reporte-de-ciberataques-en-colombia-2019-de-policia-nacional-y-ccit-428790)

- Suplantación de identidad con un 28% ocupa la segunda casilla, debido a su gran accionar tanto por vía telefónica como por internet, aprovechándose del desconocimiento o inocencia de las personas.

- Malware hace presencia con el 14% en la posición 3, viéndose un poco disminuido a causa de los antivirus, antimalware y firewall que se son cada día más utilizados en las estructuras informáticas.

- Fraudes con 16% en el cuarto puesto, sigue causando pérdidas monetarias, aunque más reducido debido a que es un delito prácticamente personalizado, que requiere estudio y seguimiento de la víctima para lograr ejecutar el plan correctamente.

Lo anterior nos debe concientizar la importancia de mantenernos actualizados, pues si conocemos la forma como operan los delincuentes, más fácil podremos prevenirlos o al menos minimizar las oportunidades de convertirnos en victimas

La revista Portafolio en un artículo propio manifiesta la estadística de la Policía en relación al Ramsonware, convirtiéndose en uno de los ataques que más dinero le genera a las diferentes organizaciones.[14] Debido a la falta de preparación y capacitación de los empleados y sobretodo de las áreas TI, ya que la gran mayoría de veces, estos ataques se hacen efectivos por falta de sentido común al momento de aplicar acciones en el ordenador, imaginando que nunca serán objeto de una hacker.

En la imagen a continuación (Figura 2. Empresas preparadas) se nota que algunas empresas aun no son conscientes de las consecuencias que puede traer el no proteger sus datos

Figura 2. Empresas preparadas


Imagen propia

- Con un 82% se nota que la gran mayoría de empresas consideran que no pueden llegar a ser víctimas de ciberataques, estando equivocados.
- Por el contrario, las empresas que ya cuentan con una protección son el 18%

La ANDI está capacitando de manera acelerada a cientos de personas para que puedan aportarle un grano a la seguridad de las empresas, pues entre más personas conozcas sobre el tema mayor será la defensa a favor de la protección de los datos y los activos en general, a su vez estos nuevos conocedores de laseguridad informática están en la obligación de difundir este conocimiento en los sitios donde trabajan y familiares.

14. Portafolio, “El secuestro informático desangra a las empresas del país”, {En línea}, {29 de enero del 2019} disponible en: (https://www.portafolio.co/negocios/empresas/ciberataques-a-las-empresas-en-colombia-525729)

Colombia es uno de los países con más víctimas de ciberataques en Latinoamérica, manifiesta la revista Dinero, demostrando que existen alrededor de cuarenta y dos billones de ataques en tan solo tres meses, entre denunciados y no registrados, esto a causa de la facilidad que se presenta para adquirir y posteriormente implementar herramientas de explosión de vulnerabilidades.[15] la gran mayoría de estos software son de condigo libre y de muy fácil acceso, además se encuentran tutoriales en páginas famosas como Youtube, Facebook y otras. Se cuenta también con Sistemas Operativos como Kali Linux que ofrece de forma gratuita alrededor de trecientas herramientas para hallar debilidades pero que son también usadas para hacer intrusiones o recopilar información de las víctimas.

En la próxima imagen (Figura 3. Virus hallados) se identifica:

- Los troyanos mandan la parada en los ataques con un 87%, a causa de su fácil creación y propagación, siendo muy difícil de detectar y eliminar
- Virus varios con el 13%, también son utilizados, mas no son suficientemente eficientes como para una mayor implementación.

Figura 3. Virus hallados

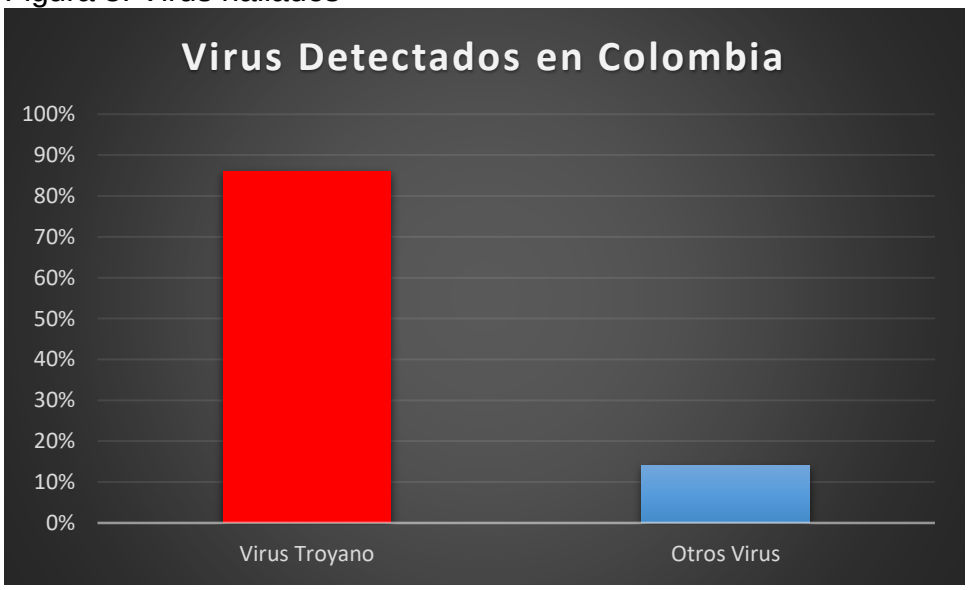



Imagen propia

En otras palabras, se puede decir que los ataques están al alcance de cualquier persona, la cual ya no requiere ir a una universidad a adquirir conocimiento, puede ser un autodidacta tan solo viendo videos e indagando en foros de hackers.

15. Dinero, “En solo tres meses Colombia sufrió 42 billones de intentos de ataques cibernéticos”, {En línea}, {05 de septiembre del 2019}, disponible en: (https://www.dinero.com/actualidad/articulo/cuantos-ataques-ciberneticos-recibe-colombia/276556)

El portal La Republica en un comunicado informa que en Colombia hay un margen de 15 horas para detectar un ataque.[16], tiempo suficiente para que un hacker capacitado y con amplia experiencia, obtenga la información que requiera, la utilice y borre el registro de todo el proceso, una vez más queda demostrado que en nuestro país nos falta amucho, tanto en tecnología como en pericia para detectar a tiempo estos delitos, no obstante hay oportunidades donde los delincuentes no son tan expertos y dejan huellas para llegar a ellos como Ip, numeración Mac, Correos y otros, obviamente son muy pocos los que permiten generar esta ruta que conlleva a la captura. La Universidad el Rosario realizo un estudio donde arrojo que el ochenta y uno por ciento de las empresas en Colombia utilizan internet, volviéndose en un blanco fácil a la hora de accionar un código malicioso. [17], siendo este medio el principal puente para ingresar un malware, ya sea por archivos maliciosos, portales falsos, cookies, extensiones, aplicaciones infectadas, etc., la red es un aporte inmenso a la hora de expandir una empresa, brindando gran cantidad de opciones, oportunidades y comunicación a nivel mundial.

En la imagen (Figura 4. Empresas que usan internet) se analiza que el 81% de las empresas utilizan internet, en cambio el 19% aun no lo hacen

Figura 4. Empresas que usan internet

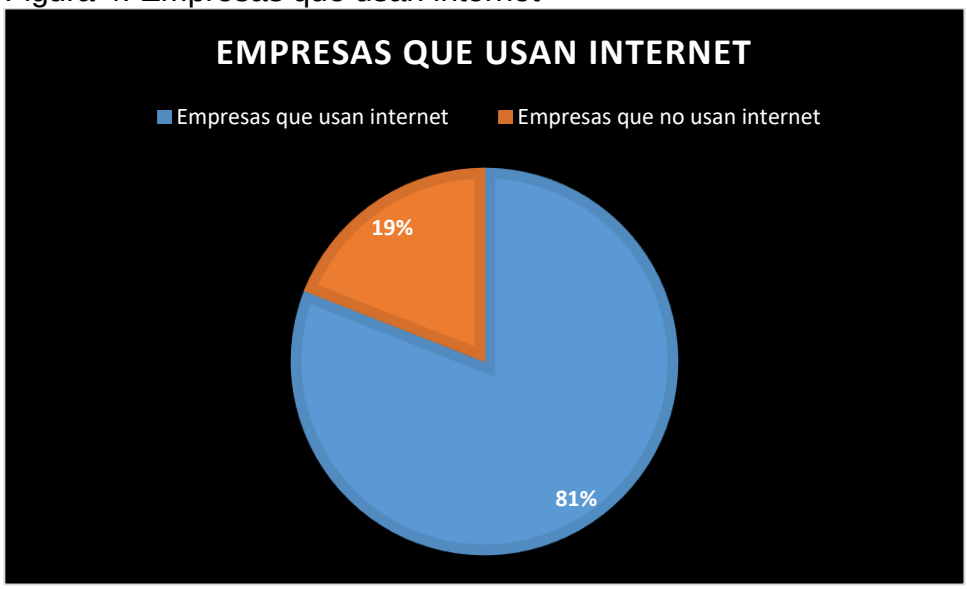



Imagen propia

16. Colprensa, “Colombia fue uno de los países con más ataques cibernéticos el año pasado”, {En Línea}, {21 de julio del 2019}, disponible en: https://www.larepublica.co/empresas/colombia-fue-uno-de-los-paises-con-mas-ataques-ciberneticos-el-ano-pasado-2887401
17. Urosario, “Los códigos maliciosos nos acechan”, {En línea}, {21 de noviembre del 2017}, disponible en: https://www.larepublica.co/empresas/colombia-fue-uno-de-los-paises-con-mas-ataques-ciberneticos-el-ano-pasado-2887401

La revista Semana escribe en su página que a nivel mundial existen muchos países que hacen su mayor esfuerzo por implementar medidas de seguridad contra los ataques hacia la información, pero por otro lado también hay otros sitios que poco o nada le prestan atención a este flagelo como es Nigeria.[18], nuestro país se encuentra en esta medida en la posición 39 de 60 analizados, siendo esto una alerta para todos, especialmente para las empresas que manejan datos delicados o portales de pago, es por esto que algunas organizaciones invierten más dinero en seguridad que en otra cosa, pues a la raga no es un gasto, es una aporte, que les brinda confiabilidad ante los clientes y sobretodo evitan perder dinero o ir a la banca rota por causa de un ataque.

En la imagen (Figura 5. Móviles infectados) se detalla, el primero (Japón), el ultimo (Nigeria) y la posición de Colombia en la lista, si comparamos se ve que aún falta mucho trabajo para lograr estar a nivel de los primeros países con mayor protección a la información, por esto no hay que desfallecer y continuar investigando, leyendo, aprendiendo y profundizando en temas como Ethical hacking. De 60 países vemos que:

- Nigeria (África)  28% infectados
- Colombia (Suramérica)  12.5% infectados
- Japón (Asia) 1.3% infectados

Figura 5. Móviles infectados

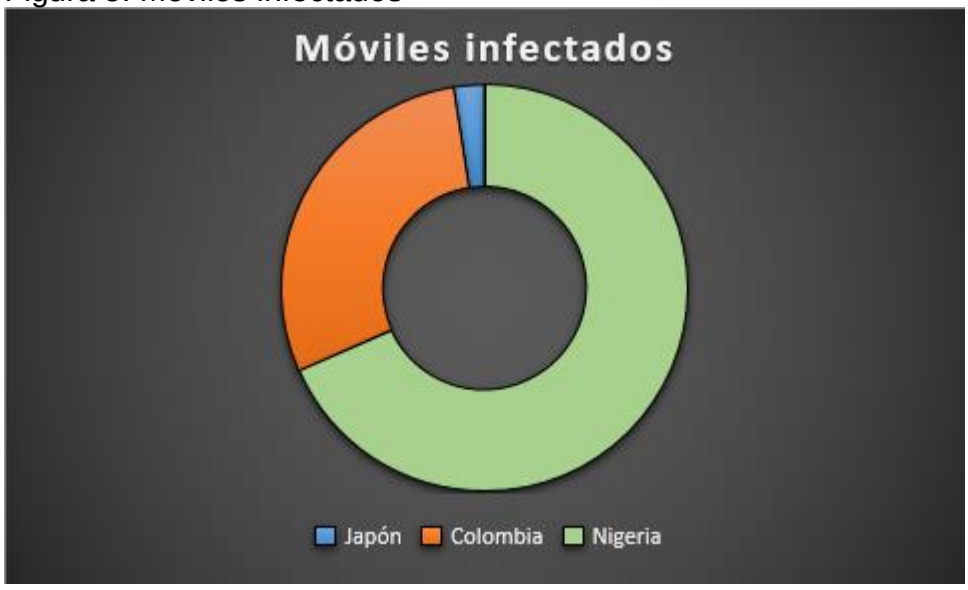



Imagen propia

18. Semana, “Así esta Colombia en el ranking de ciberseguridad mundial”, {EN línea}, {13 de febrero del 2019}, disponible en: https://www.semana.com/nacion/articulo/asi-esta-colombia-en-el-ranking-de-ciberseguridad-mundial/601118

El portal Computer World realizo una investigación, la cual arrojo que hacia el futuro la mayor cantidad de ataques serán orientados a la Nube, buscando acceder a toda la información que se almacena y gestiona en internet, por el simple motivo de que cada día las empresas dependerán más y más de estos servicios.[19], habiendo incluso empresas completamente virtuales, sin ni siquiera una oficina o un sitio físico, más que un par de ordenadores y desde ahí realizan todas las actividades y procedimientos propios de la entidad, 100% aliado con la red.

La emisora la W, realizo un reporte dado por la empresa IBM, quien expresó en un comunicado que al día en Colombia se enfrentan alrededor de 500 incidente de seguridad registrados por este pionero en seguridad.[20], esto hace referencia a entidades, empresas o individuos que tiene contratada la seguridad de sus sistemas con IBM, declarando como incidentes, no solo a ataques directos de delincuentes, sino también, errores cometidos por empleados, como es olvidar realizar respaldos de la información y la estructura tecnológica, lo cual afecta directamente a toda la empresa, perdiendo información vital para la toma de decisiones y apoyo al crecimiento de la misma.

El periódico digital El País en su Web, realizo un aporte a la seguridad informática, aconsejando la utilización de aplicaciones de monitoreo en tiempo real que permitan detectar, alertar y corregir cualquier amenaza que se presente en la parte digital o física de los sistemas.[21], también llamados IDS, son softwares pagos o de código libre que se instalan y analizan los paquetes de datos que fluyen por la red, verificando lo que ingresa sale, las direcciones IP que no vayan a ser falsas, certificados de autenticidad, rendimiento de los equipos físicos otras opciones que pueden ser configuradas por el administrador, como lista blancas

19. Computerword, “Amenazas a la ciberseguridad en el 2020”, {En línea}, {05 de diciembre del 2019}, disponible en: (https://computerworld.co/amenazas-a-la-ciberseguridad-en-el-2020/)
20. W radio, “Mas de 70 mil millones de eventos de seguridad se atienden al día”, {En línea}, {01 de junio del 2019}, disponible en (https://www.wradio.com.co/noticias/actualidad/mas-de-70-mil-millones-de-eventos-de-seguridad-se-atienden-al-dia-ibm/20190601/nota/3910044.aspx)
21. Sanchez. C, “Control en tiempo real de miles de dipositivos”, {En línea}, {26 de noviembre del 2019}, disponibl en: (https://elpais.com/economia/2019/11/20/actualidad/1574249204_860924.html)

La empresa de seguridad Eset en su reporte anual, identifico que en 2017 surgieron muchas nuevas variedades de ataques, especialmente de Ramsonware en Latinoamérica, señalando que el crimen no se estanca, esta constante evolución o mutación, tomando partes de otros similares.[22], de igual forma debe comportarse los expertos en seguridad informática, implementando diversas aplicaciones y metodologías que permitan optimizar la protección, intercambiando conocimiento con peritos en este tema de distintas partes del mundo.
En la imagen a continuación (Figura 6. Ramsonware detectados) se especifica por país, los tipos de Ramsonware encontrados, donde Colombia presento 140 tipos de ataques tipo Ramsonware, 64 menos que México

Figura 6. Ramsonware detectados

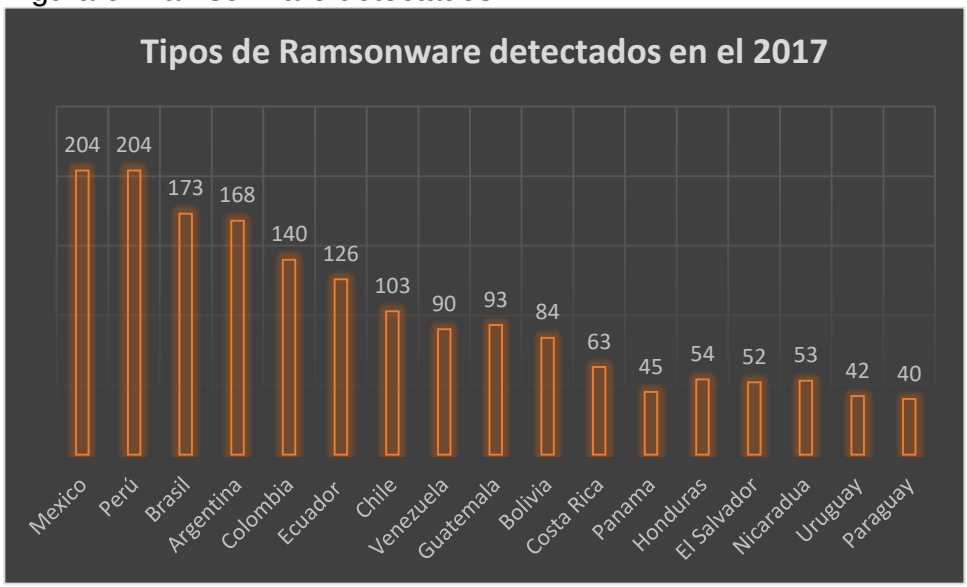



Imagen propia

Es ahí donde los equipos CSIRT o áreas TI, deben indagar y obtener información, no solo de los ataques vigentes en su país, sino también los ocurridos en los alrededores, es como ir un paso delante de este flagelo, detalle:

- México 204
- Perú 204
- Brasil 173
- Argentina 168
- Colombia 140
- Ecuador 126
- Chile 103
- Guatemala 93
- Venezuela 90
- Bolivia 84
- Costa Rica 63
- Honduras 54
- Nicaragua 53
- El salvador 52
- Panamá 45
- Uruguay 42
- Paraguay 40

22. Esete, “Eset security report Latinoamérica”, {En línea}, {01 de septiembre del 2018}, disponible en: (https://www.welivesecurity.com/wp-content/uploads/2019/07/ESET-security-report-LATAM-2019.pdf)

Karspersky señalo a través del portal el Universal que existen agencias estructuradas y establecidas únicamente para crear código malicioso como es el caso de GandCrab, que a pesar de haber “cerrado” realizo mucho daño, dejando infinidad de aplicaciones dañinas en la red.[23], igual que este grupo existen muchos otros en todo el mundo, con acceso casi ilimitado a hardware avanzado que permite cometer intrusiones fácilmente. Se podría decir que el contrapeso de estos grupos delincuenciales son los CSIRT o CERT, quienes están conformados por personal capacitado en diferentes áreas de la seguridad informática.

El portal digital Enter, divulgo hace unos meses un reporte de la Policía Nacional de Colombia, donde dicen que la mayor forma de hurto de dinero por medio digital es la suplantación de identidad, ya sea de una empresa o persona.[24], casos que se presentan casi a diario o a quien nunca le ha llegado al correo un mensaje de algún supuesto banco, manifestando que se ha bloqueado la cuenta o que es necesario ratificar unos datos, teniendo en cuenta que no tiene ninguna relación con esa entidad, esto es también llamado Phishing, a pesar de que ya es voz populi que es falso, siguen cayendo personas, quienes inocentemente brindan toda la información personal y al poco tiempo se dan cuenta que sus cuentas bancarias están vacías o sus tarjetas de crédito a reventar de compras.

La Universidad Libre realizo un análisis detallado cerca de la criminalidad informática en este país, arrojando como resultado que los delitos le apuestan Phishing, debido a su facilidad al actuar y la gran variedad que hay.[25], teniendo en cuenta que este estilo de fechorías también se está ejecutando en los últimos años por vía telefónica (SMS o llamada), conocido como Vishing pero básicamente es lo mismo, haciéndose en muchos casos desde las prisiones y con Sim Card desechables, actuando y desapareciendo sin dejar rastro.

23. Efe, “Secuestro de datos en aumento”, {En línea}, {20 de agosto del 2019}, disponible en: (https://www.eluniversal.com.co/tecnologia/secuestro-de-datos-sigue-en-aumento-HC1598229)
24. Arias. D, “Colombia, el país con más Ramsonware en Latinoamérica en 2018”, {En línea}, {15 de mayo del 2019}, disponible en: (https://www.enter.co/especiales/empresas/colombia-ataques-ciberneticos-18/)
25. Unilibre, “Crecen los ataques de Phishing en Colombia”, {En línea}, {10 de septiembre del 2019}, disponible en: (http://www.unilibre.edu.co/bogota/ul/noticias/noticias-universitarias/424-crecen-los-ataques-de-phishing-en-colombia)

La Cámara colombiana de informática y telecomunicaciones enseño en su página un reporte de la Fiscalía donde dicen que en Colombia en los últimos tiempos se han presentado perdidas entre 120.000.000 a 5.000.000.000 de pesos en diferentes organizaciones, por supuesto entre más desarrollada sea la empresa así mismo son sus pérdidas.[26], desafortunadamente muchas entidades creen que gastar dinero en la seguridad de la información es  inútil, hasta que se dan cuenta que han perdido el doble o más por incidentes tecnológicos.

Como se nota en la imagen (Figura 7. Ciudades con más denuncias informáticas) las acusaciones informáticas realizadas formalmente ante la Policía o Fiscalía son:

- Bogotá 5308 casos
- Cali 1190 casos
- Medellín 1186

Figura 7. Ciudades con más denuncias informáticas

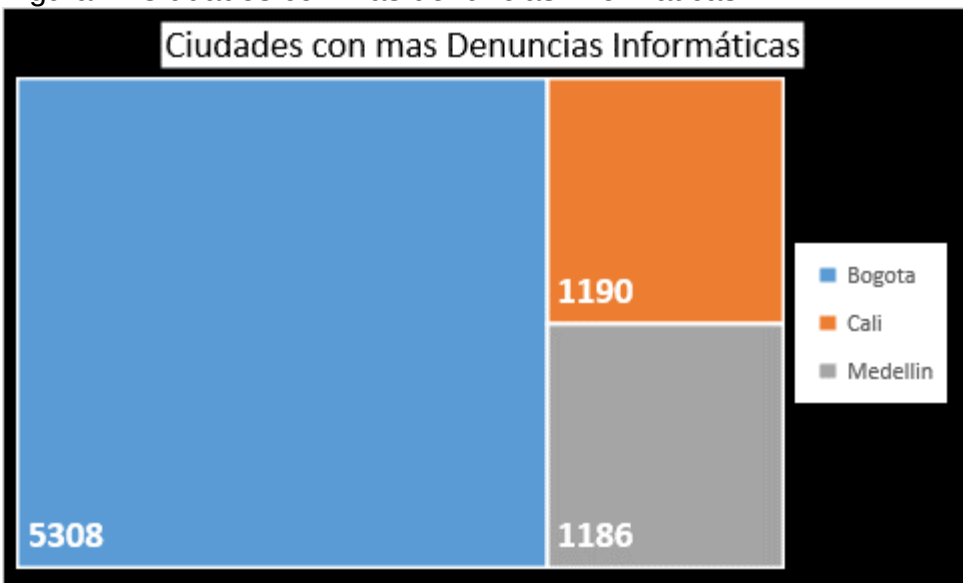



Imagen propia

Es de notar que Bogotá por ser capital y tener más empresas posee más riesgos y siempre estará propensa a incidentes de seguridad informática, mas no deja de ser un número extremadamente alto para una ciudad de aproximadamente 7.200.000 habitantes, estamos hablando de que una persona de cada 1.300 fue atacada, que se conozca pues muchas prefieren no divulgar por miedo al señalamiento o a perder credibilidad e integridad ante sus clientes

26. Tic Tac, “Tendencia del cibercrimen en Colombia 2019-2020”, {En línea}, {octubre del 2019} disponible en: (http://www.ccit.org.co/estudios/tendencias-del-cibercrimen-en-colombia-2019-2020/)

El grupo empresarial Telsys Group en su preocupación por dar a conocer e instruir a personas en todo el mundo, publico en su portal una serie de recomendaciones para incrementar la seguridad informática en las empresas y a nivel personal.[27], consejos tan sencillos como no entrar a sitios de dudosa reputación o brindar información personal, pero aunque parezca obvio, no lo es, ya que muchos jóvenes nunca se detienen a leer portales que enseñen a proteger, la gran mayoría lo único que busca en diversión y entretenimiento, (juegos, pornografía, redes sociales, etc.) y desgraciadamente estos sitios son los más contaminados, inyectando código malicioso sin que el usuario se entere, sumándole a esto los perjuicios que puede traer cuando se encuentran con personas que se están haciendo pasar por niños para engañas y cometer crímenes más delicados. Aquí es donde deben de entrar los padres a tomar un papel más activo, verificar que hacen sus hijos, con quien hablan, en que sitios navegan y sobretodo cuáles son sus amistades digitales, es necesario hablar con ellos y enseñarles los peligros a que se pueden enfrentar cada vez que ingresan a la Web.

La división de Broadcom Symantec dio a conocer un nombre en el medio informático, el FormJacking, consistente en aplicaciones que se adhieren a portales bancarios (similar a un Keylogger), registrando toda la información de las personas que ingresan a estos.[28], por lo anterior es que es tan importante la utilización de un Firewall, IDS, AntiMalware o en su defecto un Antivirus, además de mantener actualizados todas las aplicaciones como navegadores, sistemas operativos y otros. Ataques como este le pueden costar a la empresa y clientes miles de millones de pesos, pudiendo llevarlos hasta la quiebra, softwares como este no diferencian entre grandes o pequeños, obtiene información por igual, permitiendo al hacker realizar las transacciones que desee hasta que no quede dinero en las cuentas, este código malicioso se dio a conocer en el 2018 afectando a casi 5000 sitios Web y copiando los datos de aproximadamente trecientas ochenta mil tarjetas de crédito

27. Telsys, “El 85% del tráfico web empresarial se utiliza para los servicios cloud”, {En línea}, {30 de agosto del 2019}, disponible en: (https://www.telsysgroup.com.co/category/ciberseguridad/)
28. Symantec, “FormJacking”, {En línea}, {02 marzo del 2017}, disponible en: https://www.symantec.com/es/mx/security-center/threat-report

El periódico El Espectador en su portal Web relaciono una noticia ocurrida en Ucrania conocida como Black Energy con Colombia, entrevistando distintas fuentes como Karsperky lab, Eset, tratando de verificar si es podía ocurrir aquí.[29], este ataque consiste en dejar sin electricidad un país entero, provocando la caída de sistemas, servidores, internet y todos los dispositivos que no se encontraban conectados a una UPS, hecho que ocurrió el 23 de diciembre del 2015, a un día de la navidad, los representantes de estas dos entidades reconocidas por sus avances en seguridad manifestaros que de acuerdo a la tecnología que se utiliza actualmente en nuestro país, si es posible que ocurra, todo depende del compromiso de las empresas industriales en maximizar todos los medios que puedan para proteger sus activos de posibles intrusos, sean internos o externos.

La empresa de telefonía Tigo, analizando todas las víctimas de ataques cibernéticos que se han presentado en los últimos meses a través de medio de comunicación, ha colocado en su portal unas recomendaciones para evitar convertirse en víctima y como identificar si ya está siendo atacado.[30], datos que pueden ser de gran ayuda para los usuarios de los equipos tecnológicos y más aún si tienen niños pequeños, llama la atención que se enfatiza no tanto en las empresa, sino en las personas como tal, previniéndolas para cuidar todos los datos que tenga almacenado o que fluyan por la red, ya que no siempre el atacante busca obtener dinero, hay ocasiones en que desea obtener mensajes que pueden ser del correo, WhatsApp u otros, para desprestigiarlos como ya se ha visto en campañas electorales, también se puede presentar que busquen videos para enviarlos por internet y terminar con la reputación de una persona, para los cuales, los usuarios o personas que manipulan los equipos informáticos son los principales objetivos y a su vez se convierten en el punto más débil de la estructura tecnológica.

29. Ojeda. D, “¿Puede un hacker dejar sin luz a Colombia?”, {En línea}, {02 de noviembre del 2018}, disponible en: (https://www.elespectador.com/tecnologia/puede-un-hacker-dejar-sin-luz-colombia-articulo-821696)
30. Tigo, ¿Cómo prevenir los fraudes y ataques informáticos?, {En línea}, {14 de mayo del 2019}, disponible en: (https://ayuda.tigo.com.co/hc/es/articles/360036218893--C%C3%B3mo-prevenir-los-fraudes-y-ataques-inform%C3%A1ticos-General)

El portal colombiano Eje21 declaro en su portal un análisis realizado a los gerentes de las áreas TI, arrojando datos interesantes y comunes como: que la mayoría, sin dudarlo manifestaba que el éxito de los ataques en Colombia se debe a la falta de experiencia en este ámbito, además del bajo presupuesto que se asigna a esta actividad, agregaron que es difícil encontrar personas expertas en este tema y debido al auge de los avances tecnológicos, cada día va a ser más difícil.[31], se podría decir que una de las áreas más necesitadas de profesionales va a ser y es esta, la seguridad informática.

Un equipo de investigación en unión con la Policía Nacional genero un documento donde muestra hacia dónde va la criminalidad digital, mostrando estadísticas precisas de las amenazas presentes en este momento.[32], como la cantidad de denuncias formales que se hacen en Colombia y un aproximado de cuantas no lo hacen, este estudio permite enfocar todo el esfuerzo en los principales flagelos que amenazan y se convertirán en un riesgo tangible en poco tiempo.

En la imagen (Figura 8. Delitos informáticos castigados) se puede verificar la efectividad en la labor Judicial, así:

Figura 8.Delitos informáticos castigados

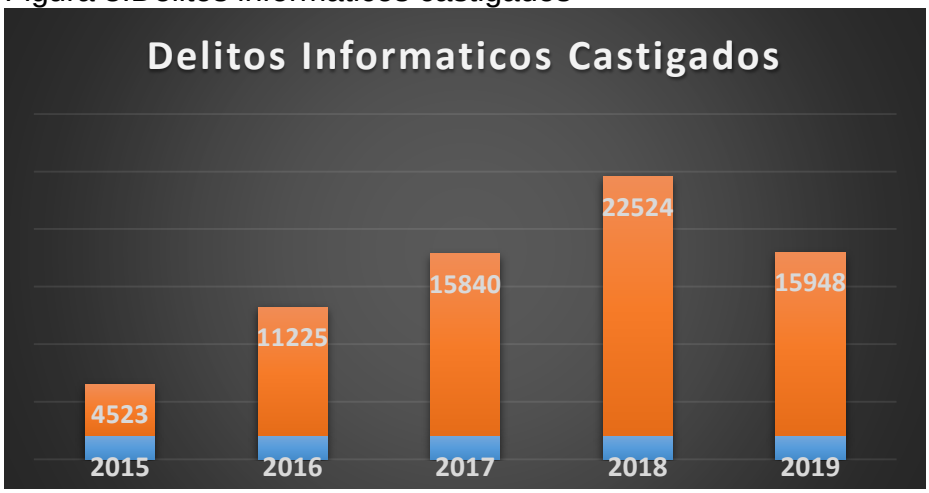



Imagen propia

31. Eje21, “Mayoría de ataques cibernéticos en Colombia provienen de sitios web maliciosos”, {En línea}, {21 de julio del 2019}, disponible en: (https://www.eje21.com.co/2019/07/mayoria-de-ataques-ciberneticos-en-colombia-proviene-de-sitios-web-maliciosos/)
32. CCIT,”Informe tendencias criminales”, {En línea}, {29 de octubre del 2019}, disponible en: http://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf

Datos de  mayor importancia en Colombia:

- En el año 2015 fueron sentenciadas 4.523 personas  en todo el país, comenzando a dar frutos  las investigaciones policiales.
- En el 2016 aumentaron los casos resueltos por los jueces a 11.225, superando a casi tres veces al año anterior.
- En el 2017 las cifras se escalaron a15.840 casos resueltos,  notándose ya el mayor accionar delictivo.
- En el 2018 se ejecutaron la mayor cantidad de castigos, entre penas y multas con una cantidad de 22.524 sumarios aplicados
- Ya en el año 2019  la suma de redujo a 15.948 casos, posiblemente a la eficiencia investigativa.

De acuerdo a los análisis realizados en este documento se pude resumir que Colombia siendo un país en crecimiento se ve muy enfrentado a los delitos informáticos, con tendencia a incrementarse cada día más, a pesar de contar con la ley 1273 del 2009 e innumerables grupos orientados a la seguridad como la policía Nacional, Fiscalía, CSIRT, CERT, áreas TI, no dejara de ser una problemática que afecte a toda la comunidad de manera directa o indirecta, esto debido al incremento y desarrollo que van teniendo los ataques, mejorando su estrategia, tecnología y códigos.

Aquí es donde entra el compromiso de todos, vinculando tanto a los expertos en seguridad informática como a los usuarios que manipulan algún dispositivo tecnológico, buscando el compromiso y la concientización de todos y cada uno, de igual forma las empresas deben entender la importancia de proteger sus activos, invertir capital y tiempo en generar barreras que detengan o mitiguen al máximo los ataques y el daño provocado por ellos.

EL Estado ha incrementado estrategias para contrarrestar esta conducta y ha tenido resultados, como se ve en la imagen anterior, además ha capacitado personal y asignado responsabilidades para tratar de ir si no un paso adelante, al menos a la par de los hackers que ponen en vilo a muchas de sus víctimas, por otro lado, también ha creado portales donde se facilitan las denuncias, las cuales son indispensables para capturar y hacer seguimiento a estos delincuentes.

EL Estado ha incrementado estrategias para contrarrestar esta conducta y ha tenido resultados, como se ve en la imagen anterior, además ha capacitado personal y asignado responsabilidades para tratar de ir si no un paso adelante, al menos a la par de los hackers que ponen en vilo a muchas de sus víctimas, por otro lado, también ha creado portales donde se facilitan las denuncias, las cuales son indispensables para capturar y hacer seguimiento a estos delincuentes.

Empresas de seguridad como Eset, Karspersky, Mcaffe y otras, dedicadas 100% a combatir los delitos cibernéticos y proteger la información, han creado labs o grupos que brindan gratuitamente soporte y recomendaciones a miles de personas en la Web, solo es compromiso de todos para buscar, leer e implementar las medidas que allí se encuentra, como se dice por ahí, es compromiso de todos.

## 7.2. ESTRUCTURACIÓN DE SERVICIOS OFRECIDOS POR EL CSIRT

Esquematizar de forma detallada los servicios en prevención y corrección de seguridad que prestara el CSIRT.

### 7.2.1. Taxonomía de Ataques Informáticos en Colombia

Para realizar un completo análisis de los incidentes realizados en Colombia se hace necesario hacer una taxonomía (división de acuerdo a una serie de características), que faciliten entender y tener una visión más orientada hacia un tipo de ataques, en la actualidad no se cuenta con un solo tipo de clasificación, por ende, se pueden hallar investigaciones más específicas o generales de acuerdo a los resultados arrojados por cada investigador

#### 7.2.1.1. Objeto de Análisis

Para una correcta taxonomía es necesario especificar que todo este estudio va orientado a la Seguridad Informática en Colombia, pasando por los diferentes incidentes presentados y las categorías de aseguramiento de la información como confidencialidad, disponibilidad e integridad (características que permiten definir si los datos son seguros)

#### 7.2.1.2. Amenazas contra la información

En la actualidad se presentan múltiples eventos que pueden atentar contra los activos, los cuales pueden ser:

##### 7.2.1.2.1. Según su intencionalidad

- Voluntarios, causados por personas que lo realizan de forma deliberada
- Involuntarios, son realizados de forma espontánea, sin deseo de hacer daño alguno

##### 7.2.1.2.2. Según su origen

- Naturales, causados por desastres naturales (terremoto, incendio, inundación, etc.)
- Artificiales, generados por personas

#### 7.2.1.3. Clasificación de los Delitos Informáticos

En la categorización de los diferentes ataques se han tenido en cuenta las principales tipologías se cada uno, tratando de hacer grupos que puedan ser una viva representación de ellos, teniendo en cuenta que cada día surgen nuevos incidentes y muchos otros simplemente mutan o se asocian entre sí.
Algunas de las principales clasificaciones son:

##### 7.2.1.3.1. Según los términos que los define

Esta categoría se basa en el detalle del significado de cada ataque, verificando que es, como funciona y como se evita, entre otros están los DoS, software ilegal, delitos contra la distribución ilegitima, troyanos, etc.

##### 7.2.1.3.2. Según sus cualidades

Aquí entra la estructura de cada ataque, se tiene en cuenta que lo conforma de acuerdo a un estudio detallado, permitiendo entrar aquí algunas divisiones como:

- Hurto de password
- Ingeniería social
- Fallas del sistema

- Errores de comprobación
- Cambios en los protocolos
- Intrusión a los datos
- Insuficiencia de servicios

#### 7.2.1.3.3. Según las consecuencias que causan

En esta opción se tiene en cuenta los efectos que generan los ataques luego de ejecutarse y pueden ser:

- Cambios no permitidos
- Desvío de datos
- Hardware, software o servicios no disponibles

#### 7.2.1.3.4. Según la dimensión

Con esta clasificación se tiene en cuenta de donde viene el riesgo, así:

- Vulnerabilidad, es más la acción que el quien
- Posible agresor, quienes tienen accesos a los equipos y a la información

#### 7.2.1.3.5. Según su objetivo

Dicha clasificación se orienta de acuerdo a la nacionalidad del ataque y son:

- Perturbación, impide que el sistema fluya con claridad
- Apropiación, obtiene daos o una información especifica
- Edición, cambia los datos o el funcionamiento del sistema
- Creación, genera un nuevo dato o una acción nueva en la estructura

#### 7.2.1.3.6. Según el procedimiento que ejecuta el ataque

Categoría que se basa en identificar el medio que utiliza el malhechor para ejecutar la acción ilícita, junto con todos los pasos, está conformada por:

- Agresor, puede ser interno (de la misma empresa) o externo (no tiene nada que ver con la organización)
- Instrumentos, son todas las herramientas que utiliza durante el ataque
- Vulnerabilidad, por donde ingresa el ataque, el camino o debilidad.
- Consecuencias, los efectos causados por la agresión.
- Propósito, objetivo del ataque

### 7.2.2. Catálogo de Servicios

#### 7.2.2.1. Servicios Reactivos

Los servicios reactivos son aquellas acciones que se ejecutan al momento de alertar o detectar un incidente, obligando a actuar lo antes posible y con las medidas ya establecidas con anterioridad, así:

1. Crear alertas que permitan avisar de la acción lo antes posible.
   A través de un monitoreo del sistema con aplicaciones IDS que pueden detectar una amenaza antes de que ejecute su ataque.
   En este momento el principal IDS(sistema de detección de intrusos) utilizado en el mercado es Snort, estos brindan información oportuna y alarmas instantáneas referentes a diferentes amenazas como son exploits, análisis de paquetes, falsos positivos, seguimiento al entorno de la red, ataques DOS, VOIP, NetBios, en general brinda un entorno seguro para la empresa y toda la información que manipulen, junto con la estructura tecnológica de la misma, por último, permite configurarse de acuerdo a las necesidades de cada cliente.
   También se cuenta con IPS (Sistema de prevención de intrusos), con este software se refuerza la seguridad informática en la entidad, frenando la inserción de códigos maliciosos y la creación de puertas traseras en el sistema, de acuerdo a la configuración pueden ser:
   - Orientado a firmas, apoyándose de códigos identificados de ataques pasados y registrados en su base de datos.
   - Orientado en error, monitoreando fallas o situaciones fuera de lo común que se presenten en el sistema.
   - Orientado en reglas, las cuales se detallan teniendo en cuenta las funciones requeridas por la organización.
   - Orientado como anzuelo, tomando datos que permitan crear barreras a futuro para detener estos ataques.

   Un administrador del CSIRT verifica el comportamiento del entorno tecnológico de la empresa, haciendo un seguimiento constante y en tiempo real de cada comportamiento que se presente, analizando y realizando las acciones necesarias para mantener la seguridad de los activos. Siempre con la mayor discreción y confidencialidad que ameritan estas instancias.

2. Estandarización de la administración de incidentes
   El CSIRT cuenta con un protocolo pre establecido con los procedimientos a

realizar al momento de presentarse un incidente, ya sea accidental o voluntario, entre ellos:

- Utilizar correctamente los dispositivos de hardware y software para que estén preparados en caso de presentarse una anomalía, a l igual que el personal de usuario del sistema.
- Previamente se realiza un estudio de toda la estructura del sistema, sus componentes y funcionamiento detallado, creando documentos y respaldo que permitan conocer si se ha presentado algún cambio.
- Activación y configuración de los aplicativos de monitoreo y prevención de incidentes de acuerdo a los requerimientos del sistema y del cliente.
- Al momento de presentarse un incidente, se realiza un análisis para identificar de que tipo es y que alcance puede tener (triaje), teniendo en cuenta sus características, entorno de operación, funcionamiento y todo lo que pueda aportar a la eliminación o mitigación del mismo, tomando las acciones necesarias al respecto para enfrentar la situación con toda la responsabilidad que amerita, siempre apoyado por un experto con amplio conocimiento y con las herramientas necesarias para detener el incidente y crear las salvaguardas necesarias para que no vuelva a presentarse, dejando un registro completo de lo ocurrido y las acciones que se tomaron.
- Se realizar pruebas de seguridad para constatar que el incidente ya no está presente y se aplican mejoras al sistema teniendo en cuenta la experiencia obtenida.
- Posteriormente se hace una valoración de lo sucedido, verificando que tipo de impacto presento, se le asigna una clasificación teniendo en cuenta su tipología, se califica la actuación del CSIRT, contando el tiempo de respuesta y el daño ocasionado.
- Por último, se genera un informe formal del incidente y se envía al grupo de CSIRT y CERT para tenerlo en cuenta y no se presente en otras organizaciones.

3. Analizar correctamente los incidentes
   El equipo está compuesto por funcionarios con bastante conocimiento y certificados que analizaran el incidente detalladamente para identificar las acciones a seguir, contando con bases de datos de situaciones pasadas propias y de otras entidades, así mismo se manejan estándares que facilitan las acciones a seguir. Las herramientas que se utilizan, aplicaciones de

seguridad, monitoreo, hardware y personal, se mantienen en constante actualización para ir a la vanguardia de los incidentes informáticos a nivel nacional e internacional.

También para un correcto análisis se cuenta con políticas de seguridad, procedimientos definidos, estándares de seguridad informática local y global, así mismo se brindará capacitación al personal que manipula o hace parte de la estructura tecnológica de la empresa.

Siempre en pro de trabajar mancomunadamente tanto la empresa cliente como el CSIRT.

4. Respuesta a cualquier incidente personalmente, ya sea a propósito o accidental

   Se atiende al llamado de los clientes 24/7, atendiendo cualquier suceso que se presente, es decir, siempre hay personal disponible para acudir a cualquier llamado en todo momento, además, constantemente se pasa revista y se analiza el funcionamiento del entorno de sistemas para constatar que todo ande bien, lo anterior va de la mano con los reportes que generan a diario los sistemas de monitoreo (Sistema de Detección de Intrusos y Sistema de Prevención de Intrusos).

   También se tiene una línea telefónica correo electrónico, portal Web y oficina física para soporte técnico, dudas respecto al funcionamiento de las aplicaciones o preguntas que se generen respecto a la seguridad informática y constantemente se realizan charlas o conferencias para capacitar al personal que se relacione o contrate con la compañía caso de estudio Cybersecurity Colombia LTDA.

5. Apoyo técnico frente a los incidentes

   De acuerdo a los parámetros ya establecidos por la empresa caso de estudio Cybersecurity Colombia LTDA, a través del CSIRT de la misma entidad, se seguirán los pasos para controlar, eliminar o mitigar cualquier incidente que se presenten el menor tiempo posible y con las mejores herramientas y personal perito en el tema.

   Buscando en todo momento brindar un servicio eficiente y de calidad, demostrando responsabilidad, amplio conocimiento y el deseo firme de proteger los activos de los clientes.

6. Reglamentar las respuestas a los sucesos

   El CSIRT se apoya bajo una normatividad legal que le permite actuar con parámetros legales vigentes como:

Nacionales

- ICONTEC, Instituto colombiano de normas técnicas y certificación
- MinTic, Ministerio de las TICs
- CNTV, Comisión nacional de televisión
- CRC, Comisión de regulación de comunicaciones
- Sistema nacional de normalización, certificación y metrología,
- CIDET, Corporación centro de investigación y desarrollo tecnológico

Internacionales:

- ISO, Organización internacional de normalización
- IEEE, Instituto de ingenieros eléctricos y electrónicos
- NIST, Instituto nacional de estándares y tecnología
- OMG, Grupo de administración de objetos
- TIA, Asociación de la Industria de las Telecomunicaciones
- ANSI, El Instituto Nacional Estadounidense de Estándares
- OSI, Modelo de interconexión de sistemas abiertos
- CEN, Comité europeo para la estandarización

7. Administrar las vulnerabilidades informáticas que tenga la empresa
   Luego de identificar las vulnerabilidades, se aplican las medidas necesarias para corregirlas. Para una correcta protección de la información y de los activos en general de una organización, lo primero que se debe realizar es identificar las debilidades que presenta, para así, comenzar por corregirlas y cerrar posibles puertas traseras o brechas de seguridad.
   Para esto se aplican metodologías reconocidas a nivel mundial como son Magerit V3, ISO y otros, los cuales detallan los activos de la empresa y las vulnerabilidades correspondientes, de esta forma, se podrán realizar salvaguardas que corrijan a tiempo cualquier riesgo que esté presente.

8. Realizar los estudios y categorizar las vulnerabilidades
   Las vulnerabilidades detectadas son analizadas detalladamente, realizándoles un tratamiento que cubra todas las posibles fallas en el sistema, teniendo en cuenta que estas debilidades se pueden presentar en el software, hardware, la red y el recurso humano.
   Verificación que se aplicara en diferentes tiempos para incorporar dispositivos, cambios en el sistema y personal nuevo en la empresa, as se contara con una protección completa y robusta a toda la empresa.

9. Tomar acciones frente a las vulnerabilidades
   Luego de corregir las vulnerabilidades se aplican procedimientos para verificar si las acciones de mejoramiento funcionaron, llevando un control permanente del sistema, aplicando auditorias completas de tipo caja negra y caja blanca.

10. Aplicar instrumentos que permitan evitar o reducir las vulnerabilidades.
    La utilización de herramientas con PenTesting son indispensables en la verificación de procedimientos, creando un entorno controlado del sistema (virtual), se pueden hacer pruebas de penetración a los componentes de la estructura a través de aplicativos y sistemas operativos orientados a la seguridad informática, de esta manera no se afecta el sistema principal, ni se tiene que detener para hacer pruebas.

#### 7.2.2.2. Servicios Proactivos

Las acciones proactivas son aquellos servicios que se aplican en todo momento, es como ir un paso adelante a los diferentes ataques que se presenten por cualquier medio, así:

1. Documentar de forma específica todo el proceso
   Cada procedimiento que se ejecuta por parte del CSIRT se archiva, con toda la información minuciosa del caso (antes, durante y después del incidente), permitiendo usarse como antecedente y compartir el conocimiento con otros grupos similares, evitando así que esta problemática se presente de nuevo con el mismo cliente.

2. Mantener supervisión de la estructura tecnológica
   EL monitoreo del sistema se realiza de forma lógica y física constantemente al sistema, por parte del personal que integra el CSIRT, convirtiéndose en un guardián de los activos de la empresa, permitiendo esto identificar alguna anomalía a tiempo.

3. Realización de auditorías constantemente
   Las auditorias son indispensables en la detección de vulnerabilidades y verificación de cambios en el sistema, reconociendo si algún dispositivo o configuración está generando inconvenientes o abriendo brechas de seguridad que puedan ser aprovechadas por alguna amenaza, contando

siempre con el consentimiento de las directivas de la organización que contrata el servicio.

4. Monitoreo de la parte lógica y física de la seguridad
   CSIRT implementa aplicativos que mantienen una mirada a cada acción que se ejecuta en el sistema, a través de softwares diseñados y configurados para este tema, ofreciendo un servicio óptimo y analítico de acuerdo a los requerimientos presentados por parte de la estructura del sistema, identificando incidentes en tiempo real.

5. Procedimientos para evitar inserciones ilegales
   Con la ejecución de softwares de seguridad se puede controlar la interceptación de información o cualquier otro tipo de ataque lógico a o físico contra los activos tecnológicos de la empresa, como son IDS, IPS, Firewall, antivirus, servidores y configuraciones que aporten a la seguridad.

6. Compartir datos sobre seguridad
   Intercambio de conocimiento con otros entes orientados a la protección de activos, es decir, crear convenios con otros CSIRT, CERT y grupos TI para brindar y recibir experiencias vividas, permitiendo obtener conocimiento y tomar acciones que incrementen la seguridad de la información.

#### 7.2.2.3. Servicios Adicionales

El CSIRT cuenta con otros servicios que pueden ser de gran ayuda al momento de prevenir un ataque o proteger la información, aumentando el control dentro de la empresa, así:

1. Gestión de riesgos
   Identificación, corrección y salvaguardas que mitiguen o eliminen algún riesgo a los activos, permitiendo llevar un control completo de todo el esquema tecnológico de la organización.

2. Administración de negocio y salvaguardas
   La gestión en el negocio es apoyada y orientada al cumplimiento de los objetivos estratégicos, creando una línea que conlleve al cumplimiento de las metas institucionales, así mismo las medidas de remediación evitan perdida de información o caídas prolongadas del sistema.

3. Análisis de seguridad
   Auditorías externas e internas que arrojen el nivel de SGSI con el que cuenta la empresa, apoyándose de estándares de seguridad como ISO 27001 con la unión de los controles de la norma ISO 27002

4. Concientización del accionar delictivo y como protegerse
   Capacitación al recurso humano de la organización para reconocer las fallas de seguridad que se pueden presentar ocasionadas por ellos, por atacantes tanto expertos como aficionados o por fallas del hardware o software.
   Así mismo se ofrecen actualizaciones con los últimos ataques.

5. Capacitación en seguridad.
   Entender que es la seguridad y como se puede apropiar este evento para toda la entidad, concientizando a cada integrante de la organización que para una completa protección de los activos se necesita del apoyo y compromiso de todos, haciendo que cada uno se convierta en un líder en seguridad informática en la empresa y en la vida cotidiana.

## 7.3. COMPETENCIAS LABORALES DEL CSIRT

Precisar los perfiles y requisitos que deben cumplir los integrantes del núcleo laboral que harán parte del CSIRT.

### 7.3.1. Composición Interna del CSIRT

- Director del equipo
  Encargado de dirigir y verificar el cumplimiento de todas las actividades y procesos que cumple cada integrante del equipo, llevando un riguroso control y lista de chequeo que le permita hacer un análisis acerca de los objetivos de del equipo

  Lista de chequeo para el control del personal:
  - ✓ Cumple con los parámetros establecidos por los valores corporativos.
  - ✓ Asiste a las capacitaciones para mejorar su perfil laboral.
  - ✓ Aplica el conocimiento adquirido.
  - ✓ Efectúa eficazmente las tareas que se le asignan.
  - ✓ Ejerce los roles de liderazgo, compañerismo e innovación.
  - ✓ Complementa sus labores con el desarrollo personal.

- ✓ Aporta a los objetivos institucionales.
- ✓ Respeta el entorno laboral propio y de los demás.
- ✓ Demuestra confidencialidad en los procedimientos.
- ✓ Es proactivo en la protección de los activos.
- ✓ Manifiesta seguridad en la corrección de incidentes.
- ✓ Analiza correctamente los incidentes asignados.

La lista de chequeo de los procedimientos informáticos se realiza de acuerdo a la metodología, estándar o buena práctica que se aplique a la estructura tecnológica, por ejemplo, si es la norma técnica de calidad ISO 27001 se regirá con los controles de la ISO 27002, siempre a modo de auditoria, para identificar posibles fallas que se puedan presentar o implementación de ejercicios de mejoramiento.

- Equipo técnico

  Personal altamente capacitado y con experiencia en parámetros de seguridad informática, cuya misión es ejecutar los diferentes procedimientos y técnicas que conlleven a prevenir, corregir o mitigar amenazas que puedan generar un riesgo para los activos de los clientes de la empresa, aplicando una supervisión constante al hardware, software, la red y el personal que opera los sistemas de información.

  Además, tiene una relación directa con los clientes y realiza vigilancia constante con las herramientas de monitoreo para identificar en tiempo real cualquier cambio sospechoso en el sistema.

  Perfil requerido:

  - ✓ Conocimiento de las herramientas y dispositivos que se utilizan.
  - ✓ Certificación en los estándares que ofrece la empresa.
  - ✓ Identificar errores en la aplicación de los procedimientos de seguridad.
  - ✓ Familiarización con los posibles incidentes que se puedan generar.
  - ✓ Habilidades para actuar bajo presión.
  - ✓ Destrezas para resolver problemas.
  - ✓ Empatía, respeto y cautela hacia los compañeros y clientes.
  - ✓ Trabajo en equipo.
  - ✓ Habilidades metódicas
  - ✓ Formación técnica o profesional en áreas tecnológicas.
  - ✓ No tener antecedentes judiciales.

  El equipo técnico está compuesto por una unidad operativa de alrededor de

6-8 personas, de acuerdo a la capacidad laboral requerida, buscando siempre que haya un especialista en comunicación, informática, seguridad, redes, programación y servidores.

A su vez, este equipo tiene un supervisor técnico, que es el encargado de asignar funciones y gestionar la integración de cada procedimiento entre sí, teniendo línea directa con el director del equipo, ejerciendo como un supervisor y cumplimento labores administrativas.

- Analistas

  Este componente hace el estudio detallado de cada incidente que se presenta, en el menor tiempo posible, de forma rápida y metódica, definiendo las principales características del hecho ocurrido.

  Especificaciones que deben detallar de los incidentes:

  - ✓ Examina si fue voluntario o accidental.
  - ✓ Identifica posibles causas.
  - ✓ Detalla vulnerabilidades afectadas.
  - ✓ Categoriza el incidente.
  - ✓ Determina activos afectados
  - ✓ Realiza un informe minucioso de lo ocurrido.
  - ✓ Orienta posibles acciones a tomar.
  - ✓ Crea nuevas doctrinas.
  - ✓ Mantiene línea directa con otros CSIRT, CERT y grupos Ti.
  - ✓ Brinda apoyo administrativo al equipo técnico.

  Este grupo de personas son la primera línea de acción frente a un incidente, ofreciendo su amplio conocimiento en beneficio de la protección de los activos de las diferentes organizaciones que contratan con la empresa caso de estudio Cybersecurity Colombia LTDA.

  Perfil de un analista:

  - ✓ Amplio conocimiento en metodologías y políticas de seguridad.
  - ✓ Habilidades de síntesis.
  - ✓ Destrezas comunicativas.
  - ✓ Rigor con sus procedimientos.
  - ✓ Disposición constante.
  - ✓ Detallista con sus análisis.

- ✓ Conceptualizar.
- ✓ Objetividad.
- ✓ Confidencialidad con los procesos del CSIRT.
- ✓ Buena redacción.

### 7.3.2. Composición General

- Grupo de publicidad y contacto con la ciudadanía
  Genera campañas agresivas en diferentes medios, como internet, televisión, radio, BTL, voz a voz, folletos, etc. para darse a conocer, también brinda información referente a los servicios que ofrece la empresa, incluyendo costos, planes, tiempo, clausulas y demás datos llamativos que permitan obtener clientes.
  Este grupo permite que las personas y las empresas en general conozcan quienes somos, que hacemos y como lo hacemos, con esto, no solo se incrementan los ingresos, sino también aumenta en índice de seguridad de la información a nivel global.
- Persona de enlace
  Verifica y analiza los requerimientos o necesidades de las organizaciones que desean contratar los servicios del CSIRT a través de la empresa caso de estudio Cibersecurity LTDA., conviene la forma de contratación que se realiza y comienza el proceso de aplicación de servicios acordados.
  También, recibe las quejas y reclamos por parte de los usuarios, referentes a los servicios pactados, gestionándolos y aplicándoles los protocolos requeridos para darles una pronta y satisfactoria respuesta, en conclusión es el puente directo entre el equipo de reacción inmediata ante incidentes de seguridad informática y los clientes en todo momento.
- Grupo de administración de incidentes
  Tienen la responsabilidad de realizar los procedimientos técnicos para eliminar o mitigar las vulnerabilidades, amenazas y riesgos y salvaguardas de la empresa, deben ser altamente capacitados, con experiencia y certificados en el tratamiento de activos.
  Dentro de este grupo esta:
  - ✓ Director del CSIRT
  - ✓ Equipo técnico
  - ✓ Analistas

- Grupo de capacitación
  Ofrecen instrucción general y específica de seguridad a clientes y propios,

investigan nuevas formas de ataques en todo el mundo para implementar las acciones de remediación por parte del CSIRT, de esta forma se mantiene una constante mejora en el conocimiento de temas relacionados a la cibernética.

Por otro lado, realiza también formación básica a entidades sin ánimo de lucro por medio de acuerdos, para apoyar de forma gratuita a personas y organizaciones que requieren de este conocimiento y no cuentan con los recursos.

- Legislador

  Especialista en derecho quien está encargado de la parte normativa y legal de las actividades que realiza el CSIRT, supervisando el actuar, los contratos y posibles situaciones que se puedan presentar o que puedan generar una falta a la reglamentación local o internacional.

  Es necesario que conozca ampliamente las leyes y normas que rigen cada procedimiento que se ejecuta, permitiendo que se desarrolle un actuar ecuánime, justo e imparcial, por parte de cada integrante del CSIRT.

  Además, apoya al grupo de enlace en relación con los contratos, quejas y reclamos, evitando que se realicen acciones en contra de la legalidad.

- Administrativo

  Lleva el control administrativo de todos los procesos del CSIRT, como:

  - ✓ Contratos, formularios, políticas, normatividad, informes, etc.
  - ✓ Atiende las líneas telefónicas.
  - ✓ Verifica y procesa los expedientes que lleguen.
  - ✓ Analiza las agendas.
  - ✓ Gestiona el archivo.
  - ✓ Realiza informes y solicitudes a otras entidades.
  - ✓ Imparte comunicados.
  - ✓ Controla los registros financieros.
  - ✓ Supervisa la administración logística.
  - ✓ Administra las hojas de vida y seguimiento del recurso humano de la empresa.

### 7.3.3. Actividades internas del CSIRT

- Gestión administrativa.
- Identificar, estudiar, actuar y crear salvaguardas.
- Categorizar y asignar las alarmas generadas en los monitores.
- Coordinar las auditorias y capacitación.

- Aplicar análisis forense a sucesos ocurridos.
- Indagar sobre actualizaciones en ataques.
- Hacer campañas de publicidad y temas de seguridad.
- Gestionar los procedimientos de réplica a incidentes.
- Crear un archivo de antecedentes de los procedimientos efectuados.
- Control de la normatividad que rige el CSIRT.
- Administrar eventos remotos de seguridad.
- Realizar informe detallado de cada procedimiento.
- Capacitarse y actualizarse constantemente en técnicas y protocolos de seguridad.
- Aportar a la mejora de la seguridad informática a nivel global.

### 7.3.4. Perfil individual de un integrante del CSIRT

- Responsabilidad
- Honesto
- Comprometido
- Analítico
- Acucioso
- integro
- Tener iniciativa
- Allegado al trabajo en equipo
- Experto en seguridad informática
- Tener más de tres años de experiencia en el tema
- Conocedor de las pruebas de penetración
- Manejo de metodologías, estándares y buenas practicas
- Buen manejo de hardware y software de seguridad
- Diestro en el uso de IDS y sistemas pasivos de monitoreo

## 7.4. POLÍTICAS Y PROCEDIMIENTOS ESTRATÉGICOS

Definir las normas, políticas, estándares y procedimientos operacionales que permitirán un normal desarrollo del CSIRT.

Para la realización y normal ejercicio del CSIRT es prioritario identificar y cumplir cada norma que cubra los diferentes procedimientos que se realizan de forma

externa o interna, siendo un ejemplo en el cumplimento y la legalidad en todo momento.

### 7.4.1. Manual Operacional CSIRT

#### 7.4.1.1. Reglas Generales

Las reglas generales son las normas que debe cumplir cada integrante del CSIRT, sin importar el cargo o la función que ejerza, las cuales se realizan en todo momento y con cualquier cliente o servicio que se preste, así:

- Cumplir con la normatividad nacional e internacional que cubra el actuar del CSIRT, junto con las leyes de protección de la información vigentes en Colombia y los contratos realizados por los clientes y la organización conforme a lo establecido en ellos.
- No violar los parámetros de seguridad que no hayan sido especificados y concertados con los clientes, además, eliminar inmediatamente se termine la auditoria los datos clasificados obtenidos en pruebas de PenTesting y metodologías de intrusión.
- Las soluciones, remediaciones y salvaguardas siempre estarán orientados a proteger los activos del cliente, siendo protector de esquemas, usuarios, contraseñas y demás información delicada del funcionamiento de la empresa.
- Antes de iniciar cualquier procedimiento en una organización se debe establecer un documento que faculte y detalle cada actividad que se vaya a realizar.
- En los procedimientos a efectuarse solo participará personal que integre el CSIRT, no se permitirá la utilización de personal ajeno a esta dependencia por ningún motivo.
- No se ejecutarán procedimientos, pruebas o demás acciones que no estén contempladas en el contrato inicial
- Siempre se terminarán las actividades con un informe minucioso dirigido a las directivas de la empresa, únicamente.
- No se realizarán comentarios, burlas o se divulgara algún dato obtenido durante las auditorias.
- El actuar del CSIRT está encaminada a buscar la integridad, confidencialidad y disponibilidad de la información

- Ningún integrante del CSIRT realizaría contratos o procedimientos por separado, sin conocimiento de las directivas de la empresa.

#### 7.4.1.2. Acciones Frente a un Incidente

Este grupo de reacción frente a incidentes de seguridad cibernética tendrá estandarizadas las funciones y la forma como actuará, definiendo los pasos a seguir, quien los realizará, buscando siempre evitar o mitigar los daños causados por ataques o accidente informáticos.

**Tareas**

- Intervenir y reducir cualquier daño que se pueda presentar en los activos de la organización
- Recopilación de muestras y evidencia referente al ataque o accidente presentado.
- Crear antecedentes documentados de todas las acciones que se tomen y de lo encontrado.
- Definir el contexto detallado del incidente, incluyendo origen, acciones, secuelas y posible culpable o generador.
- Tomar decisiones y procedimientos que permitan recuperar el sistema o corregir el daño lo más pronto posible.
- Generar alternativas y recomendaciones para que este incidente no se vuelva a presentar.
- Alimentar la base de datos de las lecciones aprendidas que sirvan como archivo de apoyo y búsqueda en futuros incidentes de la misma u otra entidad.
- Intercambiar los conocimientos y antecedentes adquiridos en las diferentes situaciones con otros CSIRT o grupos de seguridad informática.

#### 7.4.1.3. Sectores Operacionales

El CSIRT realizara acciones en diferentes campos, tanto públicos como privados, brindando un servicio eficiente y comprometido en la protección de los activos de la entidad.

- Empresas pequeñas, mediana y grandes
- Sector estudiantil
- Negocios y áreas comerciales
- Área militar

- Entidades estatales
- Organizaciones privadas

#### 7.4.1.4. Gestión de la información

Siendo conscientes que la información es el principal activo con que cuenta toda organización, se ha realizado un detallado esquema de clasificación que permita dar un control óptimo y eficiente.

**Control**

Un adecuado y sensible control de la información conlleva a incrementar la seguridad, es por esto que se debe aplicar los siguientes puntos:

- Garantizar la disponibilidad en todo momento
- Adecuados protocolos de confidencialidad
- Manipulación (envió, transporte y recepción) con estándares de seguridad
- Correcto almacenamiento
- Acceso de acuerdo a los privilegios penamente establecidos

**Categorías de privacidad**

La información es clasificada de acuerdo a las especificaciones de confidencialidad y acceso por parte de los usuarios.

- Privado – mayor grado de confidencialidad
- Limitado – acceso menos exclusivo pero no tan confidencial
- Propio – Todos los integrantes de la organización acceden
- Publico – accedo libre

**Clasificación según el tipo**

Bajo esta división se tiene en cuenta la categoría y los detalles que caracterizan cada elemento.

- Información electrónica,
- Bases de datos
- Escritos físicos
- Correos electrónicos
- Dispositivos de almacenamiento
- Información oral

#### 7.4.1.5. Protección de datos

No hay que escatimar en las medidas de seguridad que se apliquen en cuanto a proteger los datos se trate, por ende hay que tomar acciones para un correcto cuidado como son:

- Solo se debe entregar a personas confiables y que realmente la necesiten
- Su eliminación debe ser con parámetros de seguridad
- Utilizar mecanismos de cifrado
- Si los va a transportar, utilice dispositivos seguros
- No comparta usuarios, ni contraseñas
- Jamás guarde contraseñas en papeles o en sesiones
- Use contraseñas seguras (mayúscula, minúscula, numero, carácter)
- Cambie paulatinamente su contraseña
- No ingresar a redes sociales en los dispositivos de la organización
- Evite descargar archivos adjuntos de desconocidos
- No ingrese a sistemas de información desde ordenadores o redes publicas
- Omita instalar aplicaciones desconocidas
- Desconfié de todo y de todos

De igual manera todos los datos confidenciales recuperados u obtenidos en el análisis o durante las actividades propias del CSIRT, deben ser destruidos al término del servicio, dejando registrado el procedimiento en la minuta de actividades.

Así se evitara que la información antes mencionada llegue a manos inescrupulosas que la puedan utilizar para efectuar un ataque informático o un chantaje.

Al comienzo de todo servicio que se vaya a brindar, se debe realizar y firmar un contrato de confidencialidad, donde cada uno de los que allí estén registrados, estará en la obligación de no compartir, divulgar o guardar información de las organizaciones.

#### 7.4.1.6. Retención de Información

Esta política se aplicara con mucho tacto y específicamente la información netamente necesaria para archivo y posteriores búsquedas, solo retendrán los siguientes datos:

- Nombre del caso
- Fecha de inicio de la actividad
- Fecha término de la actividad
- Nombre de la empresa
- Incidentes presentados
- Actividades realizadas (general)
- Responsable de la empresa
- Responsables del CSIRT involucrados
- Informe de la gestión
- Resultados
- Contrato de servicio
- Acuerdo de confidencialidad

Con estos datos se podrá tener un registro adecuado y concluyente que pueda ser útil en procesos posteriores con la misma u otra empresa, esta información será guardada como archivo en dispositivos confiables, bajo contraseña, cifrado y solo tendrán acceso los gerentes de proceso, actuando siempre bajo la normatividad vigente en Colombia, como es la Ley 1581 de 2012 “protección de datos personales”

Todo lo anterior debe quedar claramente estipulado en el contrato de servicios, donde se estipula el consentimiento de ambas partes y se firma.

#### 7.4.1.7. Destrucción de Información

La destrucción o eliminación de la información es clave en toda organización, en especial la privada o limitada, ya que de no hacerse con los protocolos adecuados puede convertirse en una vulnerabilidad muy grande.

**Información física**

- Comprobar que el dueño de la información u otros relacionados no la necesitan
- Hacer un registro de los documentos a eliminar
- Pasar documento por el corta papel
- Recogerlo en una bolsa independiente

- Incinerarlo, ya sea por medio químico u otro, en su defecto contratar una empresa certificada para esta eliminación
- Nunca arrojarlo con la basura en general

**Información lógica**

- Eliminar de forma segura los datos
- Pasar por un campo magnético elevado el dispositivo, para dañarlo
- Triturar el dispositivo de almacenamiento
- Contratar con una empresa para la incineración de los equipos
- No se debe confiar con eliminar los datos con la tecla suprimir o formatear el dispositivo

Con lo anterior se busca que una persona no pueda volver a tener acceso a los datos, eliminando toda forma de análisis forense que se le ´pueda aplicar a la información física o lógica

#### 7.4.1.8. Divulgación De Información

El CSIRT siendo un grupo que maneja información de alto nivel de confidencialidad de las empresas, se empeña mantener la calidad de secreto con el cliente, utilizando acuerdos de confidencialidad registrados, que conlleven a evitar la divulgación de la información del cliente, concientizando a cada integrante de las consecuencias que puede acarrear el propagar datos delicados.
La empresa caso de estudio Cibersecurity de Colombia LTDA. Realiza estudios de seguridad y confiabilidad a cada integrante de la entidad, buscando que las personas que allí laboren sean integras, honestas y responsables, previniendo así cualquier fuga de información.

Cada integrante del CSIRT está en el deber de reportar y denunciar cualquier caso de divulgación de información, ya sea de los clientes o de las actividades y formas d trabajar del equipo.

La ley 1273 del 2009, en el artículo 269F, estipula la pena que acarrea quien divulgue información por cualquier método o motivo (cárcel de 48 a 96 meses, multa de 100 a 1000 SMLV)

El CSIRT divulgara únicamente información sin relevancia de los casos, con el fin únicamente académicos, los cuales conlleven a mejorar la seguridad informática de otras personas y empresas.

El equipo de reacción funda sus principios en proteger la información propia y ajena, por esto, brinda todas las garantías necearías para impedir que los datos sean divulgados.

#### 7.4.1.9. Acceso a la Información

El control del acceso a la información debe ser minucioso, ya que de esto depende una adecuada protección de los activos, para lo anterior se deben tener en cuenta los siguientes ítems:

- Asignación y seguimiento detallado de privilegios, controlando que cada persona acceda únicamente a la información necesaria para el cumplimiento de sus funciones
- Monitoreo de los despidos, vacaciones, cambios de cargo y demás situaciones que requieran un cambio o eliminación de acceso a la información
- Seguimiento de las actividades que realizan en los dispositivos de la organización, creando un registro con datos como, usuario, fecha, hora, paginas accedidas y accesos fallidos
- Mantener la información fuera del alcance de personas que no estén autorizadas para conocerla (física y lógica)
- Configurar el sistema para que las contraseñas tengan tiempo de vencimiento y solo admita claves seguras
- Asignar un responsable del monitoreo de todos los estándares de acceso de la organización
- Implementar aplicaciones de monitoreo de actividades de los usuarios
- Asignar un sitio y dispositivos seguros para el almacenamiento de la información, junto con el archivo, restringiendo su acceso

Es responsabilidad de cada integrante de la entidad, velar por el control y la protección de los accesos a la información, ya que de esto depende la seguridad de toda la organización

El control del acceso a la información no puede hacer que se pierda la disponibilidad de la misma, por ende, el análisis de privilegios debe ser muy detallado pero no restrictivo para las personas que requieran estos datos

#### 7.4.1.10. Uso apropiado de los sistemas del CSIRT

El grupo de respuesta ante incidentes de seguridad informática tiene como objetivo reducir los sucesos que generen algún riesgo en una empresa, apoyándose de herramientas, software y configuraciones adecuadas para corregir vulnerabilidades, no obstante antes de contratar un servicio con un cliente, primero se verifica que los requerimientos estén dentro de la legalidad y las funciones propias del mismo, previniendo ser manipulados para accionares ilegítimos.

Nunca se tomaran servicios informáticos que puedan conllevar a atentar contra el buen nombre, la moral y los valores de la empresa caso de estudio Cibersecurity LTDA de Colombia, además, el director de grupo mantendrá un control sobre los integrantes del equipo, verificando que su actuar sea el más integro posible, cumpliendo con todos los parámetros pre-establecidos dentro del actuar legal, evitando que las herramientas que se utilizan en el CSIRT sean usadas para fines personales.

Se ejerce un control de las licencias y certificados del software, constatando que se encuentren aplicados a los dispositivos de la organización, contándolo como un activo importante.

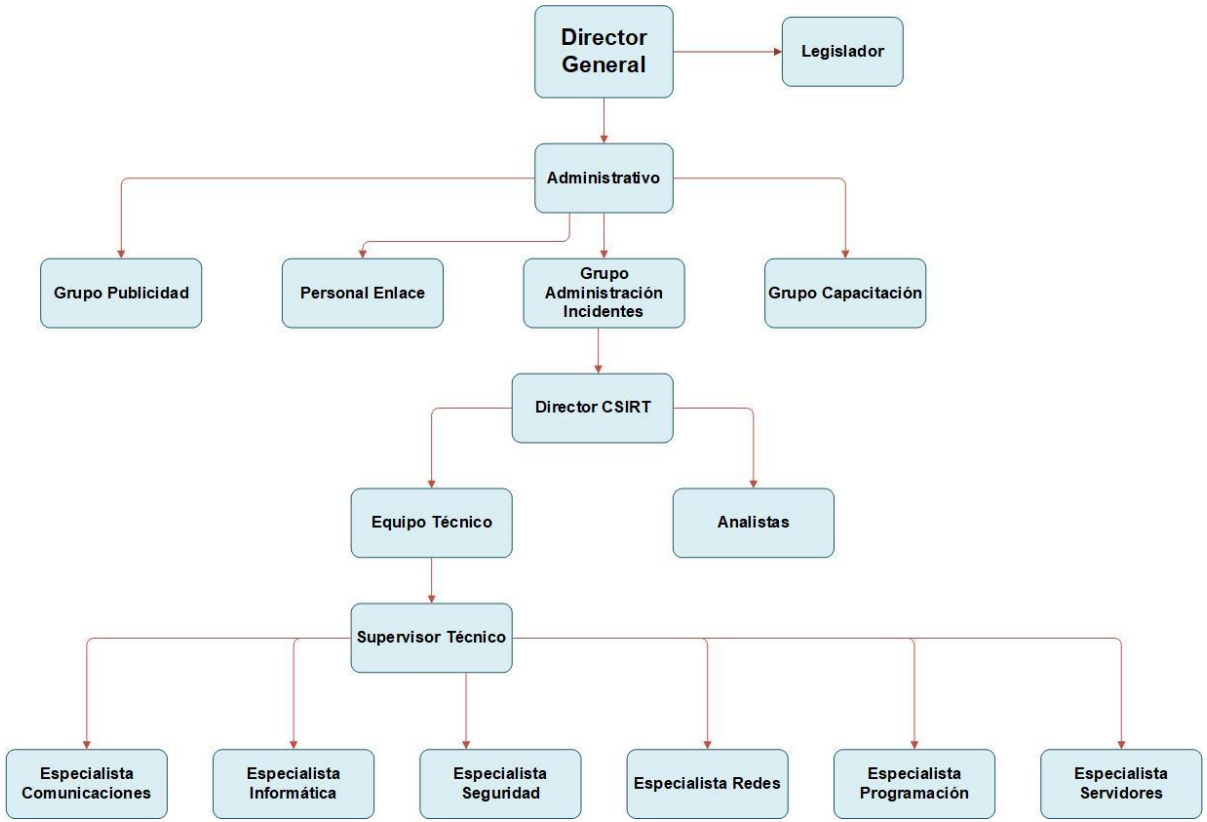
Se realizaran constantemente auditorías internas, verificando que todos los procedimientos se estén efectuando correctamente y el accionar personal sea muy transparente.

Continuamente se hacen capacitaciones de integridad en el trabajo a todo el personal de la unidad, dando a conocer y recordando los valores y los compromisos de confidencialidad y honestidad que se tienen con los clientes y con la misma organización.

### 7.4.1.11. Estructura Orgánica

En la siguiente imagen (Organigrama General) vemos la estructura completa de la entidad

Figura 9.Organigrama General




Fuente: Propia

#### 7.4.1.12. Cooperación

La definición de cooperación consiste en practicar una labor mancomunadamente ente varios grupos o personas, buscando alcanzar un objetivo común.

Llevado a la realidad, permite que varios grupos de reacción como CSIRT, CERT, áreas TI, grupos de investigación informática, creen una red de comunicación que permita intercambiar experiencia y conocimiento acerca de incidentes, tanto a nivel local como global, orientado todo a combatir los delitos informáticos y los sucesos involuntarios que puedan afectar el normal desarrollo de un sistema de información. Con lo anterior se crea un entorno de respuesta mucho más amplio y completo, que logra brindar soluciones eficientes y amplias a personas y empresas en todo el mundo, siendo los incidentes informáticos una problemática que afecta a todo el mundo.

La cooperación permite también mantener a los integrantes del CSIRT actualizados acerca de los cambios que presentan los crackers y su accionar delictivo, pudiendo generar salvaguardas mucho más complejas y eficaces para proteger los activos informáticos.

Este apoyo de conocimiento da la opción de aprender de los inconvenientes que hayan podido cometer otros grupos, ya sea por desconocimiento o falta de experiencia, en pocas palabras, aprender de los errores de otros, previniendo que estos vuelvan a suceder.

Otro apoyo importante es la cooperación interinstitucional, con entes como la Policía y la Fiscalía, brindando y recibiendo sabiduría que aporte al esclarecimiento de investigaciones cibernéticas (CSIRT Policía – Grupo de Reacción Informática de la Fiscalía).

### 7.4.2. FACTIBILIDAD DEL PROYECTO

Aplica cuando se cumple con todos los requisitos necesarios para hacer viable el cumplimiento del proyecto, teniendo en cuenta una serie de elementos o recursos indispensables para dar culminación a los objetivos plenamente establecidos.

Se debe describir previamente lo que se visualizara en la tabla y debe dársele un título.

En la tabla siguiente (tabla 1 Factibilidad) se puede detallar la problemática, junto con sus signos de identificación.

Tabla 1. Factibilidad

| **Identificación del problema** | **Signos específicos** |
|---|---|
| Incremento de los delitos informáticos de los clientes de la empresa caso de estudio Cibersecurity de Colombia LTDA | • Quejas por parte de los clientes<br>• Perdida de información<br>• Descuentos desconocidos<br>• Llamadas desconocidas |
| Requerimiento de documentos necesarios para crear un CSIRT | • Panorama actual de la ciberseguridad en Colombia<br>• Estudio de factibilidad<br>• Taxonomía de ataques relevantes<br>• Catálogo de servicios |
| Falta de servicio para dar soporte a los clientes | • Requerimientos sin respuesta por parte de los clientes<br>• Ausencia de soporte en eficiente<br>• Servicios débiles y de poca capacidad |

Fuente: Propia

#### 7.4.2.1. Factibilidad técnica

Para la ejecución de este proyecto se requieren equipos de hardware como ordenadores, servidores y demás dispositivos de conexión, los cuales son fáciles de conseguir y algunos de los cuales ya posee la empresa, demostrando que no genera ningún inconveniente para el desarrollo de esta actividad, pudiendo dar cumplimiento a cabalidad de todos los requisitos en la creación de un CSIRT

#### 7.4.2.2. Factibilidad económica

En el camino al cumplimiento de este proyecto se hace necesario cumplir con unos términos de tiempo, con el cual se cuenta por parte tanto de los funcionarios, como de las directivas, de igual forma es prescindible la compra de algunos softwares como Firewall, IDS (siendo algunos de código libre) y otros como viáticos, licencias, etc., necesarios para el control de amenazas, vulnerabilidades y riesgos, dinero ya

presupuestado y listo para su utilización. Por lo anterior se ratifica la posibilidad de la realización en este ámbito.

#### 7.4.2.3. Factibilidad operativa.

El talento humano necesario para hacer efectivo este propósito, está disponible, tanto con el tiempo, conocimiento y experiencia, también está dispuesto a colaborar en todo lo que se necesita, siendo un apoyo no solo en la elaboración de este proyecto, sino que sirven como apoyo en las áreas de amplia experiencia que manejan.

#### 7.4.2.4. Resultado de la factibilidad

Después de terminar el análisis de esta propuesta de proyecto queda definido que es factible y viable, generando confianza y una mirada clara en la consecución de las metas a donde se quiere llegar, permitiendo crear los documentos para la generación de un CSIRT, el cual será de gran apoyo no solo a la empresa caso de estudio Cibersecurity de Colombia LTDA, sino también a otras entidades y personas que se relacionan con ellos, atacando directamente el flagelo de los delitos cibernéticos y protegiendo de manera óptima los activos de las diferentes entidades.

#### 7.4.2.5. IMPACTO ECONÓMICO

Los resultados del impacto económico son favorables, dados luego de un análisis detallado de los requerimientos financieros para el desarrollo de este proyecto, así:

A. Beneficios
   - Ahorro de papel, siendo el 95% de los documentos digitales
   - Acreditación comercial, permitiendo obtener mayor cantidad de clientes
   - Mitigación en la perdida dinero por actos delictivos
   - Reducción de denuncias y reclamos por falsificación de identidad en transacciones bancarias
   - Protección de activos, alargando su vida útil

B. Costos

   Presupuesto del proyecto 63.000.000 pesos aproximadamente
   Con la tabla (Tabla 2. Presupuesto) se registra al detalle los gastos requeridos para la implementación.

Tabla 2. Presupuesto

| | |
|---|---|
| Plataforma informática | 8.000.000 |
| Gastos de operación | 15.000.000 |
| Componentes de oficina | 30.000.000 |
| Adquisición de servicios básicos | 5.000.000 |
| Capacitación | 5.000.000 |
| **Total** | **63.000.000** |

Fuente: Propia

C. Impacto económico local1

- Su principal aporte es el apoyo en la lucha contra los delitos informáticos, generando ventajas en su área de aplicación y a terceros de forma indirecta, reduciendo las pérdidas financieras de muchas personas, por medio de recomendaciones y asesoras en los portales Web.

### 7.4.2.6. IMPACTO SOCIAL

El impacto social que tendrá este proyecto se verá reflejado en empresas e individuos, brindando un grano de arena en el cuidado de la información y los activos en general, reduciendo el índice de la problemática que se nota hoy en día relacionada con los ciberataques.

También se contará un CSIRT que brindará un apoyo de servicios y soporte eficiente en tiempo real, permitiendo mantener las condiciones de integridad, confidencialidad y disponibilidad de la información, durante todo el flujo tecnológico.

En general el CSIRT será un apoyo incondicional a nivel global en el intercambio de información de incidentes, siendo un respaldo para grande y chicos que se empeñan en eliminar del todo la delincuencia informática.

### 7.4.2.7. IMPACTO AMBIENTAL

El mayor impacto ambiental está relacionado con la reducción del uso del papel, siendo una directiva global, donde poco o nada se realizará de manera física, la gran mayoría de documentos generados serán digitales, manteniendo todo el

entorno de archivo de forma lógica, alejado de contaminación y cerca de la prevención del deterioro del medio ambiente.

#### 7.4.2.8. IMPACTO TECNOLÓGICO

En esta área es donde se verá el mayor impacto, convirtiendo al CSIRT de la empresa caso de estudio Cibersecurity de Colombia LTDA. En una herramienta indispensable en contra de los incidentes que atenten contra los activos de una gran cantidad de organizaciones de todo tipo y de forma indirecta con sus familias, amigos y demás personas que se asocien con el uso de las tecnologías de comunicación.

Por otro lado, será un referente para las empresas que busquen seguir los mismos pasos en la creación de un CSIRT, todo orientado a apoyar la lucha contra los hackers que quieren terminar con la confianza en el manejo de los diferentes sistemas informáticos.

# 8. RESULTADOS

Con la tabla (tabla 3. resultados), se asigna el indicador a cada resultado propuesto

Tabla 3. Resultados

| RESULTADO/PRODUCTO ESPERADO | INDICADOR | BENEFICIARIO |
|---|---|---|
| Documento con la situación actual de Colombia en los últimos tres años respecto a la CiberSeguridad. | Cualitativo | Empresa Cibersecurity de Colombia LTDA |
| Documento con el estudio de la factibilidad del proyecto y en que entornos ejercerá el CSIRT | Cualitativo | Empresa Cibersecurity de Colombia LTDA |
| Documento con el análisis de los ataques más comunes, identificando métodos, clasificación y forma de actuar | Cualitativo | Empresa Cibersecurity de Colombia LTDA |
| Documento que especifique los servicios que se prestaran y de qué forma se ejecutaran | Cualitativo | Empresa Cibersecurity de Colombia LTDA |
| Documento que detalle los perfiles de los integrantes del CSIR, junto con sus funciones | Cualitativo | Empresa Cibersecurity de Colombia LTDA |
| Manual de políticas y procedimientos operacionales | Cualitativo | Empresa Cibersecurity de Colombia LTDA |
| Documento con la estructura orgánica del CSIRT | Cualitativo | Empresa Cibersecurity de Colombia LTDA |

Fuente: Propia

## 9. VIDEOS

A continuación se registran los links de los videos relacionados a los avances realizados en las tutorías Proyecto de Seguridad Informática I y II (2019-2020)

1. Primera fase 1
   https://www.youtube.com/watch?v=smIn840kfyg&feature=youtu.be

2. Primera fase 2
   https://www.youtube.com/watch?v=gXgOHxcR4Ns&feature=youtu.be

3. Primera fase 3
   https://www.youtube.com/watch?v=0MRnkQ4Y03s&feature=youtu.be

4. Avance proyecto de grado.
   https://www.youtube.com/watch?v=gZ9IPAYBK8Y&t=95s

5. Avance Proyecto de Grado 2
   https://youtu.be/rhajN-AfURw

# 10. CONCLUSIONES

Se crearon los documentos administrativos que permiten afianzar el Centro de Respuesta a Incidentes Cibernéticos para la empresa Cibersecurity de Colombia LTDA.

Se detalló el contexto de aplicabilidad del CSIRT, al igual que los aportes que ofrecen en la ejecución y en el cumplimiento de los parámetros de seguridad, constatando la necesidad de la creación de la documentación y complementando un profundo análisis de la situación delictiva.

Durante el proyecto se especificaron todos los servicios que ofrecerá el CSIRT, puntualizando la forma, de que tipo y como enfrentará las diferentes amenazas que se presenten.

Quedaron definidos los requisitos que deben tener los integres de este equipo, al igual que las especificaciones del perfil de cada cargo que se ejecutara dentro de la conformación del equipo de reacción.

Las políticas, estándares, metodólogas y procedimientos que regirán las actividades del CSIRT quedaron establecidas y detalladas.

# 11. RECOMENDACIONES

Este proyecto se realiza en la búsqueda de soluciones que puedan revolverse algunas de las problemáticas de la sociedad, por lo tanto, se recomienda a otras empresas implementar más Centros de Respuesta a Incidentes Cibernéticos que puedan aumentar las defensas y hacer frente a los diferentes ataques cibernéticos que se hacen y se harán en el futuro.

Otra recomendación es continuar investigando más a profundidad sobre las formas de actuar de los delincuentes informáticos, dándolas a conocer a las personas que hacen parte u operan estaciones de cómputo, despertando la conciencia de la seguridad y aplicando el sentido común en cada actividad que realicemos.

## 12. BIBLIOGRAFÍA


CISCO, “Seguridad para redes empresariales”, {En línea}. {2019} disponible en: (https://www.cisco.com/c/es_co/solutions/enterprise-networks/enterprise-network-security/index.html?CCID=cc000009&DTID=pseggl000015&POSITION=SEM&COUNTRY_SITE=co&CAMPAIGN=sc-00&CREATIVE=CO_SEM_SEC_Security-SPA_PM_NB_-ADW_All-Visitors-Seguridad-&REFERRING_SITE=Google&KEYWORD=seguridad%20informatica&ds_rl=1261909&ds_rl=1261909&gclid=Cj0KCQjwiILsBRCGARIsAHKQWLMXIyH-JjNwcyBSJFuyYAqUFF0xGUVkhURKQGivX2q6Eks7Sf8GUXIaAqKPEALw_wcB)

LA NACIÓN, “Bill Gates apuesta por un nuevo sistema de seguridad informática”, {En línea}. {2017} disponible en: (https://www.nacion.com/tecnologia/bill-gates-apuesta-por-un-nuevo-sistema-de-seguridad-informatica/RIDPAYNYANEBBI3LM5EPU3WW44/story/)

MUNDO,” Zuckerberg rompió su silencio y habló sobre el escándalo de Cambridge Analytica”, {En línea}. {2019} disponible en: (https://www.semana.com/mundo/articulo/que-dice-mark-zuckerberg-sobre el-escandalo-de-cambridge-analytic/561079)

ENISA, “Como crear un CSIRT paso a paso”, {En línea}. {2006} disponible en: (https://www.enisa.europa.eu/publications/csirt-setting-up-guide-in-spanish/at_download/fullReport)

CCN, “Guía de creación de un CERT/CSIRT”, {En línea}. {2011} disponible en: (https://www.ccn-cert.cni.es/publico/seriesCCN-STIC/series/800-Esquema_Nacional_de_Seguridad/810-Creacion_de_un_CERT-CSIRT/810-Guia_Creacion_CERT-sep11.pdf)

GUZMÁN A. Clara Lucía, “Contextualización del cibercrimen en Colombia”, {En línea}, {23 de octubre de 2009} disponible en: (https://www.researchgate.net/publication /313874979_Contextualizacion_del_Cibercrimen_en_Colombia/link/58ac5ea8aca272c47d9d3467/download).

URIBE RAYAS. Edgar Felipe, “proceso para la definición de servicios iniciales en un equipo de respuesta ante incidencias de seguridad informática (CSIRT)”, {En línea}. {17 de diciembre de 2014} disponible en: (https://cimat.repositorioinstitucional.mx/jspui/bitstream/1008/437/1/ZACTE42.pdf)

MONTILLANO VIVAS. Manuel Emilio, “Análisis y propuesta para la implementación de un Equipo de respuestas a incidentes cibernéticos (CSIRT) en el Ministerio de Ciencia y Tecnología.”, {En línea}, {diciembre de 2009} disponible en: (http://repositorio.conicit.go.cr:8080/xmlui/bitstream/handle/123456789/184/Proyecto-Final.pdf?sequence=1&isAllowed=y)

El nuevo siglo, “Casi 29 mil ciberestafas en 12 meses: Dijin”, {EN línea}, {12 de enero de 2019} disponible en: https://www.elnuevosiglo.com.co/articulos/01-2019-casi-29-mil-ciberestafas-en-12-meses-dijin

## 13. REFERENCIAS BIBLIOGRÁFICAS


1. BC. Noticias, “En 2018 se reportaron 11.529 casos de incidente informáticos en Colombia.”, {EN línea}, {14 de mayo de 2019} disponible en: (http://www.bcnoticias.com.co/en-2018-se-reportaron-11-529-casos-de-incidentes-informaticos-en-colombia/)

2. Arias. D, “Colombia, el país con más ramsonwareen Latinoamérica, 2018”, {EN línea}, {15 de mayo de 2019} disponible en: https://www.enter.co/especiales/empresas/colombia-ataques-ciberneticos-18/

3. Avast, “Malware y Antimalware”, {En línea}, {18 de octubre del 2018} disponible en: (https://www.avast.com/es-es/c-malware)

4. Wikipedia, “Tecnología Informática”, {En línea}, {28 de agosto del 2011}, disponible en: https://es.wikipedia.org/wiki/Tecnolog%C3%ADa_inform%C3%A1tica

5. CISCO, “Seguridad para redes empresariales”, {En línea}. {2019} disponible en: (https://www.cisco.com/c/es_co/solutions/enterprise-networks/enterprise-network-security/index.html?CCID=cc000009&DTID=pseggl000015&POSITION=SEM&COUNTRY_SITE=co&CAMPAIGN=sc-00&CREATIVE=CO_SEM_SEC_Security-SPA_PM_NB_-ADW_All-Visitors-Seguridad-&REFERRING_SITE=Google&KEYWORD=seguridad%20informatica&ds_rl=1261909&ds_rl=1261909&gclid=Cj0KCQjwiILsBRCGARIsAHKQWLMXIyH-JjNwcyBSJFuyYAqUFF0xGUVkhURKQGivX2q6Eks7Sf8GUXIaAqKPEALw_wcB)

6. LA NACIÓN, “Bill Gates apuesta por un nuevo sistema de seguridad informática”, {En línea}. {2017} disponible en: (https://www.nacion.com/tecnologia/bill-gates-apuesta-por-un-nuevo-sistema-de-seguridad-informatica/RIDPAYNYANEBBI3LM5EPU3WW44/story/)

7. MUNDO," Zuckerberg rompió su silencio y habló sobre el escándalo de Cambridge Analytica", {En línea}. {2019} disponible en: (https://www.semana.com/mundo/articulo/que-dice-mark-zuckerberg-sobre el-escandalo-de-cambridge-analytic/561079)

8. FIRST, "FIRST shares 11 vital steps towards cyber security resilience in 2020", {En línea}, {09 de octubre del 2019} disponible en: (https://www.first.org/newsroom/releases/20191009)

9. Molist. M, "La gente no está entrenada contra el engaño a través de la tecnología", {En línea}, {15 de junio del 2006}, disponible en: https://elpais.com/diario/2006/06/15/sociedad/1150322409_850215.html

10. Elconfidencial, "Tu coche ya está conectado a internet y ahora cualquiera puede usarlo para matarte", {En línea}, {11 de julio del 2019} disponible en: (https://www.elconfidencial.com/tecnologia/2019-07-11/bruce-schneier-ciberseguridad-iran-iot-corea-norte-click-matarlos-a-todos_2115135/)

11. Sasia. D, "Gestión de incidentes de seguridad de la información/CERT/CSIRT {EN línea}, {07 de octubre de 2015} disponible en: https://es.slideshare.net/danielsasia/gestin-de-incidentes-de-seguridad-de-la-informacin-cert-csirt

12. El Tiempo, "En 2019 se reportaron más de 28.000 casos de ciberataques en Colombia", {En línea}, {30 de octubre del 2019}, disponible en: (https://www.eltiempo.com/tecnosfera/novedades-tecnologia/reporte-de-ciberataques-en-colombia-2019-de-policia-nacional-y-ccit-428790)

13. Portafolio, "El secuestro informático desangra a las empresas del país", {En línea}, {29 de enero del 2019} disponible en: (https://www.portafolio.co/negocios/empresas/ciberataques-a-las-empresas-en-colombia-525729)

14. Dinero, "En solo tres meses Colombia sufrió 42 billones de intentos de ataques cibernéticos", {En línea}, {05 de septiembre del 2019}, disponible

en: (https://www.dinero.com/actualidad/articulo/cuantos-ataques-ciberneticos-recibe-colombia/276556)

15. Colprensa, “Colombia fue uno de los países con más ataques cibernéticos el año pasado”, {En Línea}, {21 de julio del 2019}, disponible en: https://www.larepublica.co/empresas/colombia-fue-uno-de-los-paises-con-mas-ataques-ciberneticos-el-ano-pasado-2887401

16. Urosario, “Los códigos maliciosos nos acechan”, {En línea}, {21 de noviembre del 2017}, disponible en: https://www.larepublica.co/empresas/colombia-fue-uno-de-los-paises-con-mas-ataques-ciberneticos-el-ano-pasado-2887401

17. Semana, “Así esta Colombia en el ranking de ciberseguridad mundial”, {EN línea}, {13 de febrero del 2019}, disponible en: https://www.semana.com/nacion/articulo/asi-esta-colombia-en-el-ranking-de-ciberseguridad-mundial/601118

18. Computerword, “Amenazas a la ciberseguridad en el 2020”, {En línea}, {05 de diciembre del 2019}, disponible en: (https://computerworld.co/amenazas-a-la-ciberseguridad-en-el-2020/)

19. W radio, “Mas de 70 mil millones de eventos de seguridad se atienden al día”, {En línea}, {01 de junio del 2019}, disponible en (https://www.wradio.com.co/noticias/actualidad/mas-de-70-mil-millones-de-eventos-de-seguridad-se-atienden-al-dia-ibm/20190601/nota/3910044.aspx)

20. Sánchez. C, “Control en tiempo real de miles de dispositivos”, {En línea}, {26 de noviembre del 2019}, disponible en: (https://elpais.com/economia/2019/11/20/actualidad/1574249204_860924.html)

21. Esete, “Eset security report Latinoamérica”, {En línea}, {01 de septiembre del 2018}, disponible en: (https://www.welivesecurity.com/wp-content/uploads/2019/07/ESET-security-report-LATAM-2019.pdf)

22. Efe, “Secuestro de datos en aumento”, {En línea}, {20 de agosto del 2019}, disponible en: (https://www.eluniversal.com.co/tecnologia/secuestro-de-datos-sigue-en-aumento-HC1598229)

23. Arias. D, “Colombia, el país con más Ramsonware en Latinoamérica en 2018”, {En línea}, {15 de mayo del 2019}, disponible en: (https://www.enter.co/especiales/empresas/colombia-ataques-ciberneticos-18/)

24. Unilibre, “Crecen los ataques de Phishing en Colombia”, {En línea}, {10 de septiembre del 2019}, disponible en: (http://www.unilibre.edu.co/bogota/ul/noticias/noticias-universitarias/424-crecen-los-ataques-de-phishing-en-colombia)

25. Tic Tac, “Tendencia del cibercrimen en Colombia 2019-2020”, {En línea}, {octubre del 2019} disponible en: (http://www.ccit.org.co/estudios/tendencias-del-cibercrimen-en-colombia-2019-2020/)

26. Telsys, “El 85% del tráfico web empresarial se utiliza para los servicios cloud”, {En línea}, {30 de agosto del 2019}, disponible en: (https://www.telsysgroup.com.co/category/ciberseguridad/)

27. Symantec, “FormJacking”, {En línea}, {02 marzo del 2017}, disponible en: https://www.symantec.com/es/mx/security-center/threat-report

28. Ojeda. D, “¿Puede un hacker dejar sin luz a Colombia?”, {En línea}, {02 de noviembre del 2018}, disponible en: (https://www.elespectador.com/tecnologia/puede-un-hacker-dejar-sin-luz-colombia-articulo-821696)

29. Tigo, ¿Cómo prevenir los fraudes y ataques informáticos?, {En línea}, {14 de mayo del 2019}, disponible en: (https://ayuda.tigo.com.co/hc/es/articles/360036218893--C%C3%B3mo-prevenir-los-fraudes-y-ataques-inform%C3%A1ticos-General)

30. Eje21, “Mayoría de ataques cibernéticos en Colombia provienen de sitios web maliciosos”, {En línea}, {21 de julio del 2019}, disponible en: (https://www.eje21.com.co/2019/07/mayoria-de-ataques-ciberneticos-en-colombia-proviene-de-sitios-web-maliciosos/)

31. Eje21, “Mayoría de ataques cibernéticos en Colombia provienen de sitios web maliciosos”, {En línea}, {21 de julio del 2019}, disponible en: (https://www.eje21.com.co/2019/07/mayoria-de-ataques-ciberneticos-en-colombia-proviene-de-sitios-web-maliciosos/)

32. CCIT,”Informe tendencias criminales”, {En línea}, {29 de octubre del 2019}, disponible en: http://www.ccit.org.co/wp-content/uploads/informe-tendencias-cibercrimen_compressed-3.pdf